

Arcot™ TransFort™

Issuer Software

**Administration Manual
Version 6.4.5**



455, West Maude Avenue, Sunnyvale, CA 94085-3517

TransFort Issuer Software—Administration Manual

Version 6.4.5

Publication Date: March 2008

Part Number: AT060-001DC-06400

Copyright © 2008 Arcot Systems, Inc. All rights reserved.

This manual, as well as the software described herein, is furnished under license and may be used or copied only in accordance with the terms of the license. The content of this manual is furnished for informational purposes only. It is subject to change without notice and should not be construed as a commitment by Arcot Systems.

Arcot Systems makes no warranty of any kind with regard to this manual. This includes, but is not limited to the implied warranties of merchantability, fitness for a particular purpose or non-infringement. Arcot Systems shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance or use of this material.

Except as permitted by the software license, no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means without the prior written permission of Arcot Systems, Inc.

Trademarks

Arcot, the Arcot logo, WebFort, AccessFort, TransFort, ArcotID, and “Securing e-Business Anywhere” are all trademarks of Arcot Systems, Inc.

SecureCode and MasterCard are trademarks of MasterCard. 3-D Secure and Visa are trademarks of Visa International. Other trademarks are the property of their respective owners.

Patents

This software is protected by United States Patent No. 6,170,058, 6,209,102 and other patents pending.

Arcot Systems, Inc., 455, West Maude Avenue, Sunnyvale, CA 94085-3517.

Third Party Software

The following third-party software components have been packaged with the TransFort Issuer Software:

libcurl

Copyright © 2000, Daniel Stenberg, <daniel@haxx.se>. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

OpenSSL

Copyright © 1998-2000 The OpenSSL Project. All rights reserved.

MSXML Parser 3.0

Copyright © 2000, Microsoft Corporation. All rights reserved.

Tomcat

Provided by the Jakarta Project, Apache Software Foundation.

Contents

Preface	1
About This Manual	2
Intended Audience	2
Information Included in this Manual	2
Related Publications	4
Conventions Used in This Book	5
What's new in version 6.4.5	6
Chapter 1 Introduction to Administrator Operations	7
Administrator Group Hierarchy	8
Master Administrators	8
Global Administrators	9
Issuer Administrators	9
Administrators	10
Privileges List	10
Advanced Authorization	14
Administrator Across Issuers	14
Administrator Across Levels	14
About Administrator Privileges and Password Policies	15
Dual Control	15
Administrator Password Policies	16
Getting Started with the Administrative Console	17
Administrative Console User Interface	17
Basic Administrator Tasks	19
Logging in and out of the Administrative Console	19
Changing your Administrator Password	20
Updating Your Profile	21
Exporting a Report to a File	22

Viewing the Exported File	23
Chapter 2 Managing Administrators	25
Creating Administrator Accounts	26
Creating Administrators and Issuer Administrators	26
Creating Global Administrators	27
Creating Global Administrators using the DUC	28
Updating Administrator Privileges	30
Updating Administrator (CSR) and Issuer Administrator Privileges	30
Updating Global Administrator Privileges for a Selected Global Administrator	30
Enabling/Disabling Administrators	32
Resetting Administrator Passwords	33
Configuring Administrator Password Policy	34
Configuring Administrator Privileges	36
Master Administrator Operations	37
Managing Global Administrator Accounts	37
Viewing Administrator System Access Reports	39
CSR System Access Reports	39
Administrator Report Access Log	40
Administrator Activities Log	40
Issuer Administrator Account Reports	41
Issuer Administrator Report Access Log	41
Issuer Administrator Activities Log Report	42
Global Administrator Account Reports	42
Global Administrator Activities Log	42
Global Administrator Report Access Log	43
Chapter 3 Administrator (CSR) Operations	45
About Cardholder Enrollment	46
Standard Enrollment	46
Verifying Cardholder Identity	46
Creating the Cardholder's Identifiers	46
Abridged Enrollment	47
Activation During Shopping (ADS)	47
Opt-In	48
Issuer Activation	48
Purchase Attempts	48
Managing Cardholder Accounts	49
Adding Cardholder Accounts	49
Viewing Cardholder Account Information	51
Updating the User ID	54
Locking/Unlocking Cardholder Accounts	55

Viewing the details of a particular cardholder's account	55
Updating Cardholder Enrollment Responses	56
Resetting a Cardholder's Password	57
Cancelling Cardholder Accounts	58
Receiving Promotional Emails	58
View/update Do Not Prompt	58
Changing the Locale of a Card	59
 Chapter 4 Issuer Administrator Operations	61
Configuring Issuer Parameters	62
Managing Administrators and Issuer Administrators	65
Managing Issuer Administrator Accounts	65
Managing Administrator (CSR) Accounts	65
Viewing Administrator System Access Reports	66
 Chapter 5 Setting Up Issuer Accounts	67
Pre-Setup Tasks	68
Generating the Issuer Data Encryption Key	68
Determining the Data Upload Client Passphrase	69
Obtaining the HMAC key for AAV Calculations	69
Obtaining the BIN Key Identifier*	69
Obtaining the CVV/CVC2 Key Pair Values	70
Obtaining the CVV Key Indicator	70
Obtaining the Signing Certificate	70
Obtaining the Receipt Server Information	71
Determining the crypto device supported	71
Determining the locales supported by the Issuer	72
Creating the Issuer Account Directory	72
Creating an Issuer Account	74
Updating Issuer Information	78
Creating Range Groups	80
Configuring Range Groups	81
Configuring for Range Groups only	83
Configuring for Ranges only	83
Configuring for Ranges associated with Range Groups	84
Adding Financial Institution Information to the Issuer Account	85
Updating the Financial Institution Information	93
 Chapter 6 Configuring the Enrollment Server	95
Updating the Enrollment Server Configuration	96
MIPS and IPGS Settings	96
Admin/Enrollment Server Cache Refresh	98

Actions requiring ES Cache Refresh	98
Callout Status Delimiter Settings	98
Setting Administrator Session Timeout	98
Enrollment Process Pre Setup Tasks	100
Determining AVS and CVV2 Policy for Visa Configurations	100
Address Verification Service (AVS) Policy	100
Card Verification Value 2 (CVV2) Policy	101
Determining AVS and CVC2 Policy for MasterCard Configurations	101
Address Verification Service (AVS) Policy	102
Card Validation Code 2 (CVC2) Policy	102
Configuring for a Specific Range or Range Group	103
Landing Page for Enrollment URL	104
Configuring the Enrollment Process	105
Common Tasks for enrollment process.	105
Configuring Cardholder Fields for Standard and Abridged Enrollment	106
Configuring Order for Standard and Abridged Enrollment	108
Configuring Enrollment Process Attributes	110
Configuring Cardholder Password Policy	113
Setting Issuer Questions	115
Configuring Question Policy	116
Configuring CallOuts	118
Adding CallOut Configuration	119
Updating CallOut Configuration	121
Adding CallOuts to an Issuer	121
Updating an Issuer's CallOuts	123
Customizing the Issuer's Enrollment Site	124
Customizing the ES	124
Customizing the User Interface Template	124
Customizing Enrollment Site text	125
Customizing Enrollment Site Graphics	126
Customizing ES Graphics for MasterCard Configurations	126
Customizing ES Graphics for Visa Configurations	127
Customizing Message Files	130
Configuring Forgot Your Password in ES	131
Pre-Setup Tasks	131
Configuring Hint/Response	131
Configuring Re-Enrollment	132
Resetting Cardholder Password from Issuer's Enrollment Website	132
Chapter 7 Configuring the Access Control Server	139
Updating the Access Control Server Configuration	140
Obtaining the AHS Certificates and Key	144
Adding Support for Mobile Device	145

Adding Issuer Template Customization	146
Customizing the Issuer's Client Authentication Pages	150
Customizing the CAP Graphics	150
Configuring Forgot Your Password in ACS	152
Pre-Setup Tasks	152
Configuring Hint/Response	152
Configuring Re-Enrollment	153
Resetting Cardholder Password from Issuer's Enrollment Website	153
Auto FYP	154
 Chapter 8 Configuring ADS	161
Configuring Opt-In	162
Configuring the ADS parameters	162
Data Upload	163
Configuring CallOuts	163
Setting the PAREs Status	164
Changing ES URL	164
Enrolling Secondary Cardholder during ADS	164
Configuring Issuer Activation	170
Configuring the ADS parameters	170
Data Upload	171
Configuring CallOuts	171
Adaptive ADS	172
Cancelling Adaptive ADS	174
Summary of Cardholder Shopping Experience	175
Purchase Attempts	178
Requirements of Attempts Feature	178
 Chapter 9 Issuer Software Configuration and Log Files	183
ACS Configuration File (acs.ini)	184
Communication Channels	184
Message Handler Connection Protocols	185
Database Settings	186
Thread Settings	189
ACS Log File Settings	190
ArcotACSLog.txt File Format	191
Crypto Device Settings	192
AAV Calculation and Instance Settings	193
Supporting Multiple DS Listeners	194
Starting Multiple DS Listeners	195
Message Handler Certificates	195
Setting Cardholder Personal Message during ADS	197

ACSCClient Configuration File (acsclient.ini)	198
CAP Configuration File (cap.ini)	203
Communications Configuration File (comm.ini)	205
ES Configuration File (es.ini)	207
Log File Configuration File (log.ini)	209
ES and Administrative Console Web Configuration File (web.xml)	211
Setting Session Timeout	211
Changing the ES Log File Location	212
Specifying a Backup Issuer Software Database	212
Crypto Device Settings	215
Issuer Software Log Files	217
Modifying the Enrollment Server Log Settings	218
Backing Up Configuration Files	220
 Chapter 10 Issuer Software Command Line Utilities	 221
ACSCClient	222
Refreshing ACS Cache	222
Actions requiring ACS Cache Refresh	223
Performing a Graceful Shutdown	224
Key Management	225
Transmitting the cryptographic device PIN	226
DBUtil	227
Updating the Master Key Label	227
Inserting a Backup Issuer Software Database User Name and Password	228
Using Additional DBUtil Options	229
PK11 Util	231
Usage	231
Creating Issuer encryption keys	236
Creating a Master Key	237
Creating Issuer Signing Keys	238
Creating HMAC Keys for AAV	239
Key Util	240
Usage	240
 Appendix A Setting Up Third-Party Hardware Components	 241
Setting Up the Host Security Module	242
Configuring the HSM	242
Setting Up Key Management	243
Enabling CVV Calculations	244
Enabling Chip Card Support	244
Setting Up the Hardware Accelerator	246
Setting up a Security World	246
Creating the Master Key	247

Creating the Issuer Encryption Key	248
Creating CVV keys for CAVV	248
Creating Signing Keys	249
Adding an Accelerator to the Security World	250
Adding New Issuer Keys to the Security World	250
Setting Up IBM Cryptocard 4758	251
Creating the configuration files	251
Creating the Master Key	252
Creating the Issuer Encryption Key	252
Creating CVV keys for CAVV	253
Creating Signing Keys	253
Appendix B Error Codes	255
Transaction Details Status Codes	256
Processing Errors	258
Appendix C Default Configuration File Examples	263
acs.ini Example	264
acsclient.ini Example	270
cap.ini Example	274
comm.ini Example	275
es.ini Example	276
log.ini Example	278
Appendix D Certificates Required	279
Appendix E Restarting Services	283
Actions requiring ES Restart	283
Actions requiring ACS Restart	284
Actions requiring CAP Restart	284
Refreshing ACS Cache	284
Refreshing ES Cache	285
Appendix F System Requirements Summary	287
Issuer Software Database	287
Access Control Server	288
Software Requirements	288
Hardware Requirements	288
Client Authentication Pages	289
Software Requirements	289
Hardware Requirements	290
Enrollment Server and Administrative Console	290

Software Requirements	290
Hardware Requirements	290
Servlet Redirector	291
Software Requirements	291
Appendix G Configuring Issuer Software Components	293
Access Control Server	293
Communication Channels and Database Settings	294
Timeout Parameters	295
Wait Periods	297
Threads and Connections	298
Configuring Database Failover	301
Client Authentication Pages	302
Configuring Receipts	305
Arcot Receipt Client	306
Configuring Crypto Devices	307
Appendix H Transfort Issuer Java APIs	313
verifyPassword	314
getCHProfile	314
updateCHProfile	314
Deploying Java APIs	314
Glossary	315
Index	323

Preface

Welcome to the Arcot TransFort Issuer Software Administration. This manual provides instructions on system operations for all administrator levels and contains detailed system configuration information.

About This Manual

This section describes the intended audience for this manual and lists the chapters included in the manual.

Intended Audience

This manual is intended for Global Administrators and Master Administrators who are responsible for managing other administrator accounts, setting up Issuer accounts, and for configuring and maintaining the Issuer Software. Many topics discussed in this manual are written for administrators who have the following skills: cryptography knowledge, experience with the applicable OS, RDBMS, and familiarity with Web server administration. You can see the [System Requirements Summary](#) for more details.

If you are an Administrator (CSR) or Issuer Administrator, you may want to refer to the *Arcot TransFort Issuer Software Administration Manual for CSR*.

Information Included in this Manual

This manual is organized as follows:

- [Chapter 1, “Introduction to Administrator Operations”](#) describes the Administrator group hierarchy, administrator system access privileges, and instructions for using the Administrative Console.
- [Chapter 2, “Managing Administrators”](#) describes the different tasks to create and manage the all the different levels of administrators of Issuer Software
- [Chapter 3, “Administrator \(CSR\) Operations”](#) describes cardholder enrollment in the 3-D Secure program and provides instructions on how to perform tasks specific to the Administrator group.
- [Chapter 4, “Issuer Administrator Operations”](#) describes how to configure Issuer enrollment server information.
- [Chapter 5, “Setting Up Issuer Accounts”](#) describes how to set up Issuer accounts and all the pre-setup tasks involved.
- [Chapter 6, “Configuring the Enrollment Server”](#) describes how to configure the enrollment server.
- [Chapter 7, “Configuring the Access Control Server”](#) describes how to configure the Access Control Server

- **Chapter 8, “Configuring ADS”** describes how to configure the ADS feature in Issuer Software.
- **Chapter 9, “Issuer Software Configuration and Log Files”** describes the Issuer Software configuration and log files for the different Issuer Software components. It contains descriptions of all parameters found in the configuration files.
- **Chapter 10, “Issuer Software Command Line Utilities”** describes the command line utilities included with the Issuer Software.
- **Appendix A, “Setting Up Third-Party Hardware Components”**, describes how to set up cryptographic device for the Issuer Software deployment.
- **Appendix B, “Error Codes”**, lists the error codes applicable to the Access Control Server (ACS) component of the Issuer Software.
- **Appendix C, “Default Configuration File Examples”**, provides examples of the *.ini file settings after installation.
- **Appendix D, “Certificates Required”**, lists the digital certificates required to implement the Issuer Software.
- **Appendix E, “Restarting Services”**, lists the actions after which ES, ACS and CAP services either have to be restarted or refreshed.
- **Appendix F, “System Requirements Summary”** provides a quick preview of the Issuer Software system requirements.
- **Appendix G, “Configuring Issuer Software Components”** summarizes all the parameters required to configure the components of the Issuer Software.
- **Appendix H, “Transfort Issuer Java APIs”** discusses the Java APIs used with Issuer Software.

Related Publications

This manual references the following Arcot and other external documents:

Table 2-1 Arcot Publications

<i>Arcot TransFort Issuer Software Introduction Manual</i>	This manual explains the online authentication program and how it is implemented using TransFort Issuer Software.
<i>Arcot Data Upload Tool Installation and User Manual</i>	This manual contains instructions for installing and using the Arcot Data Upload Tool for TransFort. The Data Upload Tool is used to automatically upload certain cardholder data into the Issuer Software Database.
<i>Arcot TransFort Issuer Software Installation Manual</i>	This manual describes how to install and configure the Issuer Software according to the desired deployment environment.
<i>Arcot TransFort Issuer Software Reports Manual</i>	This manual describes instructions for viewing all the reports available in Issuer Software. It also describes all the reports in detail.

Table 2-2 External Publications

<i>Host Security Module RG7000 Operations and Installation Manual.</i>	This manual describes how to install and operate the Thales e-Security RG7000 HSM.
<i>nCipher Hardware Installation Guide</i> <i>nCipher Key-Loading Solution Guide</i> <i>nCipher PKCS #11 Library User's Guide</i>	These manuals describe how to install, run and operate the nCipher payShield Hardware Accelerator.

Conventions Used in This Book

The following typographical conventions are used in this guide:

Type	Usage	Example
Bold	Screen Items	Click the Add button. The changes will be added to the database.
<i>Italic</i>	Key Words	The <i>Broadcast Service</i> must be started before the <i>Authentication Server</i> .
	Names of Publications	For more information, consult the <i>Arcot TransFort Issuer Software Installation Manual</i> .
	Emphasis	<i>Never</i> give anyone your PIN number.
Fixed-width	Command-line input or output	# <code>cd /opt/arcot</code>
	Code Samples	<code>./authproxy start</code>
	Text File Content	<code>[arcot/NetscapeCMS] host=tupelo.arcot.com endEntityPort=443 endEntityPortUsesSSL=0 agentPort=8100</code>
	File names	<code>arcot.ini</code>
<i>Italic fixed-width</i>	Variable text. Replace italic text with the appropriate substitution.	# <code>cd <i>install_directory</i> /Install.tgz</code>
	Variable portions of file names. Replace italic text with the appropriate substitution.	<code>init<i>ORACLE_SID</i>.ora</code>
Bold fixed-width	Emphasized code sample to highlight discussed topic.	<code>sub gatewayError { my (\$msg, \$errorCod) =@_ print"Content-type: text/html\n\n" ...</code>

What's new in version 6.4.5

Arcot's Transfort Issuer Software version 6.4.0 has the following new features with respect to the 6.3.0.AIX version.

- *Create Issuer* page with new features, see [Creating an Issuer Account](#) for more information on Do Not Prompt Behaviour, User Id Supported, Two Step Login Enabled field descriptions.
- Support for [Updating the User ID, View/update Do Not Prompt, Receiving Promotional Emails](#) in *Cardholder Account Inquiry* screen. See [Managing Cardholder Accounts](#) for more information on the field descriptions.
- You can update Do Not Prompt Behaviour, User Id Supported, Two Step Login Enabled field *Update Issuer* page, see [Updating Issuer Information](#) for more information.

Introduction to Administrator Operations

The TransFort Issuer Software Administrative Console is a Web-based, operation and system management tool that provides a rich set of administrative functions including cardholder enrollment configuration, security policy configuration, Issuer Software configuration, and various report options. Different groups of administrators can access different functions.

This chapter discusses the following topics:

- Administrator groups and their relationships
- Advanced Authorization
- Administrator privileges and password policies
- Using the Administrative Console and performing basic administrator tasks

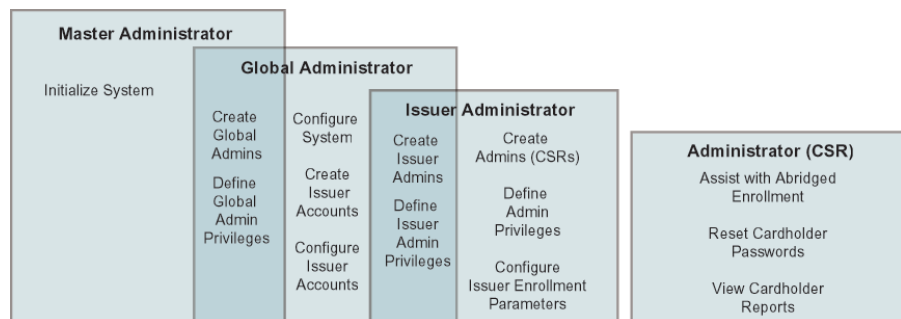
Administrator Group Hierarchy

The Issuer Software administrative functions have been distributed among four different groups of administrators. The four groups are:

- Master Administrator
- Global Administrator
- Issuer Administrator
- Administrator

This section describes each administrator role and the relationship between administrators. It also discusses Administrator privileges and password policies.

Figure 1-1 Administrator Hierarchy



Master Administrators

The Master Administrator is the highest level of administrator. The primary responsibilities of the Master Administrator are to initialize the system after installation, to create Global Administrator accounts, and to set the initial Global Administrator account access privileges.

When the Issuer Software is started for the first time after installation, two Master Administrator accounts are created to enforce dual control of the Master Administration functions. Both Master Administrators must be logged onto the system before the system will allow any changes. There will only be two Master Administrator accounts per installation (in other words, you cannot create additional Master Administrator accounts).

The list of privileges for a Master Administrator are:

- Create Global Administrator
- Configure Global Administrator Policy
- Configure Global Administrator Privileges

See [“About Administrator Privileges and Password Policies” on page 15](#) for more information on the dual control concept.

Global Administrators

Global Administrators are responsible for administering the Issuer Software. Tasks carried out by the Global Administrators include creating, managing, and modifying Issuer accounts; managing the Global, Issuer and CSR Administrator accounts; and maintaining and modifying the Issuer Software system configuration. Global Administrators can be assigned to one or more countries to provide country-specific administration support.

Master Administrators create the first Global Administrators when the Issuer Software is first set up. Other Global Administrator accounts can be created either by the Master Administrators or by Global Administrators who have been granted the privileges related to Global Administrator account creation.

Issuer Administrators

The primary responsibility of the Issuer Administrator is to manage the Administrator (CSR) accounts for an Issuer. This includes creating Administrator accounts and defining Administrator privileges. Issuer Administrators can also be responsible for managing other Issuer Administrator accounts and for configuring Issuer-specific enrollment parameters.

Global Administrators create the first Issuer Administrator accounts when the Issuer Software is first set up. Other Issuer Administrators can be created either by a Global Administrator or an Issuer Administrator granted the specific privileges related to Issuer Administration account creation.

See [Chapter 4, “Issuer Administrator Operations”](#) for detailed information on Issuer Administrator functions.

Administrators

Also known as Customer Support Representatives (CSRs), Administrators are responsible for the day-to-day operations related to cardholders who are enrolled or who are trying to enroll in the 3-D Secure program. For example, Administrators can assist with Abridged Enrollment, reset cardholder passwords, and view a variety of cardholder enrollment reports. For information on Abridged Enrollment, see “[Abridged Enrollment](#)” in [Chapter 3](#).

Administrator accounts are created by Issuer Administrators granted the specific privileges related to Administrator Account creation.

See [Chapter 3, “Administrator \(CSR\) Operations”](#) for detailed information on Administrator functions.

Privileges List

The privileges for all the administrators for the system are listed in the table below:

Table 1-1 Global Administrator Privileges

Global Administrator	Issuer Administrator	Administrator (CSR)
Configure Issuer Administrator Privileges	Update Issuer Administrator Privileges	Successful Registrations
Update Issuer Administrator Privileges	Reset Issuer Administrator Password	Reset Cardholder Password
View All Issuers	Reset Administrator Password	Update Cardholder Registration Data
Update FI Information	Enable/Disable Issuer Administrator Account	Lock/Unlock Cardholder
Global Administrator Activities Log	Configure Issuer Administrator Policy	Cancel 3-D Secure Service
Update ES Config	Create Issuer Administrator	Add Cardholder
Update ACS Config	Administrator Activities Log	Cardholder Account Inquiry
Add FI Information	Issuer Administrator Activities Log	Transaction Statistics
Create Issuer	Administrator Report Access Log	Registration Statistics
Reset Issuer Administrator Password	Issuer Administrator Report Access Log	Failed Transactions

Table 1-1 Global Administrator Privileges

Global Administrator	Issuer Administrator	Administrator (CSR)
Enable/Disable Issuer Administrator Account	Configure Issuer Parameters	Successful Transactions
Configure Issuer Administrator Policy	Configure Administrator Policy	Deactivated Cardholders
Create Issuer Administrator	Enable/Disable Administrator Account	Cardholders Added by Administrator
Reset Global Administrator Password	Update Administrator Privileges	All Registrations by Date
Enable/Disable Global Administrator Account	Create Administrator	Individual Registration Status
Update Global Administrator Privileges		Failed Registrations
Add Range Group		Upload Enrollment Data
Refresh ES/Administrator Cache		Upload Pre-Enrollment Data
Upload Enrollment Data		
Upload Pre-Enrollment Data		
Upload Admin Data		
Create Global Administrator		
Billing Information		
Update Issuer Callout		
Add Issuer Callout		
Update CallOut Configuration		
Add CallOut Configuration		
Verify Enrollment Log		
Update Issuer		
Add New Phone Support		
Add Issuer Customization		
Configure Administrator Privileges		
Reset Administrator Password		

Table 1-1 Global Administrator Privileges

Global Administrator	Issuer Administrator	Administrator (CSR)
Administrator Activities Log		
Administrator Report Access Log		
Successful Registrations		
Reset Cardholder Password		
Update Cardholder Registration Data		
Lock/Unlock Cardholder		
Cancel 3-D Secure Service		
Add Cardholder		
Cardholder Account Inquiry		
Issuer Administrator Activities Log		
Issuer Administrator Report Access Log		
Configure Issuer Parameters		
Configure Administrator Policy		
Enable/Disable Administrator Account		
Update Administrator Privileges		
Create Administrator		
Add/Update Issuer Questions		
Configure Enrollment Process		
Transaction Statistics		
Registration Statistics		
Failed Transactions		
Successful Transactions		
Deactivated Cardholders		

Table 1-1 Global Administrator Privileges

Global Administrator	Issuer Administrator	Administrator (CSR)
Cardholders Added by Administrator		
All Registrations by Date		
Individual Registration Status		
Failed Registrations		

Advanced Authorization

The hierarchical distribution of operations does not allow the administrators access across their fixed boundaries. Each level has a pre-defined privilege or role. The Advanced Authorization feature enables to create Global Administrators having all or any of the privileges of Global, Issuer and CSR administrators. Such *Enhanced Global Administrators* can perform any kind of administrative actions across Issuers without being tied down by the different levels in hierarchy. See the [Privileges List](#) for a details.

The following sections describe the different roles of the Enhanced Global Administrator:

Administrator Across Issuers

The Enhanced Global Administrator can be assigned a set of Issuers. This feature enables the administrator to operate across Issuers. There are two ways of associating an administrator with an Issuer:

1. **Creating an Global Administrator:** A list of Issuers is shown during the creation of global administrators. It is possible to select multiple Issuers. See [Chapter 2, "Creating Global Administrators" on page 27](#) for detailed instructions. The administrator thus created can operate on all the Issuers selected during creation.
2. **Creating an Issuer:** A list of all existing Global Administrators is shown when an Issuer is created. All the administrators selected and the administrator creating the Issuer will have control over the new Issuer. See [Chapter 5, "Creating an Issuer Account" on page 74](#) for detailed instructions.

An Enhanced Global Administrator should choose from a list of Issuers to do any Issuer specific operations.

Administrator Across Levels

An Enhanced Global Administrator can be defined during creation of an Global Administrator. The privilege list shown here includes the privileges of both the Issuer Administrators and Administrators (CSR's). Selecting all the privileges will enable the enhanced global administrator to perform all operations across levels.

About Administrator Privileges and Password Policies

Each administrator group has a different set of privileges. For purposes of this discussion, **privileges** are the tasks that an administrator is allowed to perform in the Administrative Console. The privileges are defined when during creation of an administrator. A global administrator defines administrator privileges and whether the tasks require dual control for Issuer administrators and Administrators (CSRs). Each administrator group (except CSRs) can set password policies for their own group and the next lower level administrator group.

The following sections describes the administrator dual control concept and administrator password and authentication policies.

Dual Control

Depending on the Issuer or processor's production policy, certain administrative tasks may require dual control. **Dual control** requires two administrators with appropriate privileges to log into the system at the same console in order to proceed with the task. Dual control stays on for the session till the second administrator explicitly logs out. The Administrative Console menu displays an asterisk (*) next to tasks that require dual control.

Master Administrators or Global Administrators with the appropriate privileges can specify dual control for specific tasks on the applicable administrator privileges pages.

NOTE:

An Enhanced Global Administrator will not require dual control for Issuer and CSR administrator privileges requiring dual control.

For information on how a Global Administrator can specify dual control, see [Chapter 2, "Configuring Administrator Privileges" on page 36](#)

For information on how a Master Administrator can specify dual control, see "[Master Administrator Operations](#)" in [Chapter 2](#).

Administrator Password Policies

Administrator password policies provide additional security protection for the administrative operations. The different levels of Administrators have jurisdiction over the next lower level administrator accounts in terms of setting password policy. For example, Issuer Administrators set the password policies for Administrators (CSRs). Configurable password policy options include password length, password format, number of failed login attempts allowed, and renewal frequency.

For information on how an Issuer Administrator can set password policy for Administrators and Issuer Administrators, see [Chapter 4, "Issuer Administrator Operations"](#).

For information on how a Global Administrator can set password policy for Issuer Administrators and other Global Administrators, see [Chapter 2, "Configuring Administrator Password Policy" on page 34](#).

For information on how a Master Administrator can set password policy for Global Administrators, see [Chapter 2, "Master Administrator Operations" on page 37](#).

Getting Started with the Administrative Console

This section describes the Administrative Console user interface and basic Administrator tasks that are universal to all Administrator groups.

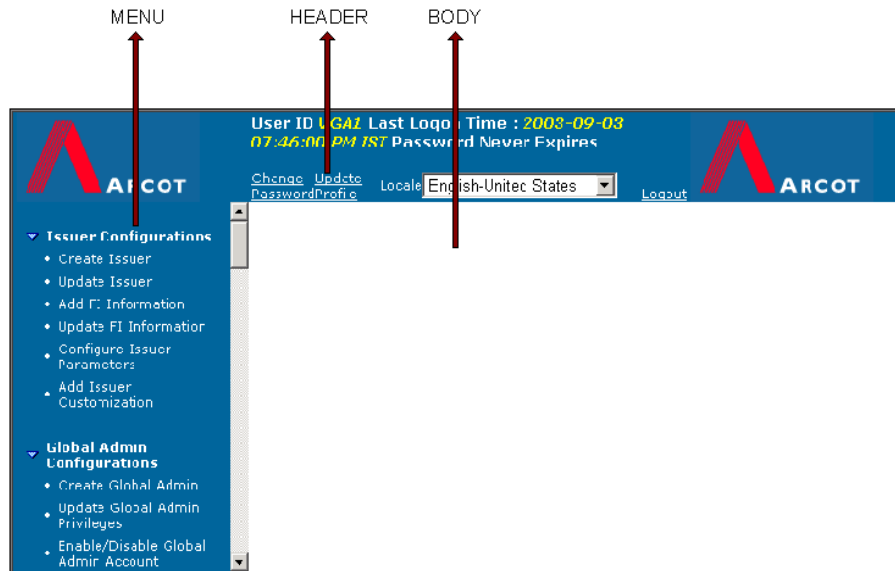
Administrative Console User Interface

The Administrative Console used by all Administrator groups has the same user interface. The user interface is composed of a three-framed view:

Table 1-2 Administrative Console User Interface

Frame	Description
Header	<p>Displays branding logos, logon information, and links to administrator-specific tasks.</p> <p>The login information includes the User ID of the administrator who is currently logged on, the time the logon occurred, and the number of days in which the administrator's password will expire.</p> <p>The header also displays a field labelled Locale which contains the preferred language of the administrator. Use the drop down menu to select the preferred locale.</p> <p>Additionally, if a second administrator is logged on (for tasks requiring dual control), the second administrator's User ID is displayed in a field called Secondary User ID.</p>
Menu	<p>Displays the action and report menu links (or privileges) available for the current administrator.</p>
Body	<p>Displays the task page for the selected menu option.</p>

The following figure diagrams the placement of the frames.

Figure 1-2 Administrator Interface Layout and Components

The Administrative Console uses the following navigation conventions:

Table 1-3 Administrative Console Navigation Conventions

Link or Button	Function	Location of Link or Button
Cancel	Cancels any user input and displays a blank body page.	Located in the Body frame of applicable function pages.
Export	Displays a “Save As” window that allows you to export report data in Comma Separated Value (CSV) format. See “Exporting a Report to a File” on page 22 for further information on this feature.	Located in the Body frame of applicable report pages.
[<<Previous] 1 2 3 [Next>>]	Scrolls through different pages of an online report.	Located on the left side immediately above and beneath the contents of a report.
Submit	Processes the current task or displays the information you are requesting.	Located in the Body frame of applicable function pages.

Basic Administrator Tasks

All Administrator groups, except where indicated, can perform the following Administrator-specific tasks:

- Log in and out of the Administrative Console.
- Change your Administrator Password
- Update your Profile*
- Export a report to a file*

The following sections provides instructions on how to perform these tasks.

Logging in and out of the Administrative Console

The following procedures describes how to log in and out of the Administrative Console. Obtain the applicable administrator URL from your Global Administrator or other system administrator prior to performing this procedure.

To log in to the Administrative Console (all administrators except Master Administrators):

1. Open a Web browser.
2. Enter the applicable Administrative Console **URL**.

The default Administrative Console URL for Administrators (CSRs) and Issuer Administrators is:

```
https://<%machine_name%>/vpas/admin/adminlogin.jsp?bank=IssuerDir
```

Where the *IssuerDir* is the name of the Issuer account folder created by the Global Administrator when setting up the Issuer account. For more information, contact the Global Administrator responsible for managing the Issuer Software.

The default Administrative Console URL for Global Administrators is:

```
https://<%machine_name%>/vpas/admin/adminlogin.jsp
```

The applicable *Administrator Login* page appears.

3. Type your Administrator **User ID** and **Password** in the applicable fields and click **Submit**.

The initial Administrative Console page appears.

**.Master Administrators do not have access to any reports in the system. Hence they cannot configure any report profiles.*

To log in to the Administrative Console (Master Administrators only):

1. On the Windows **Start** menu of the designated local Master Administrator machine, choose **Programs | TransFort Admin | Master Admin Login**.

NOTE:

Master Administrators are restricted to logging in to the Administrative Console from the machine on which the ES & Admin Console is installed. Arcot recommends using Arcot WebFort to enable remote login.

The *Master Administrator Login* page appears. This login requires both Master Administrators to be present.

2. Enter the **first Master Administrator password** in the applicable field, then have the second Master Administrator enter the **second Master Administrator password** in the applicable field.
3. Click **Submit**.

The initial Administrative Console page appears.

To log out of the Administrative Console:

- In the Administrative Console, click the **Logout** link located in the upper-right corner of the Header frame.

The system logs you out and displays the *Administrator Login* page.

NOTE:

If two administrators are logged on for tasks that require dual control, the secondary administrator should logout via the **Logout Secondary** link when the task is completed. Otherwise, the secondary administrator remains logged on until the first administrator logs out.

Changing your Administrator Password

Upon logging in to the Administrative Console for the first time, you may be required to change your password. Additionally, your administrator account may have been set up so that your password expires after a specific time interval (for example, every 60 days). In these cases, you will need to change your password when prompted. Otherwise, you may change your password as desired. The password must conform to the password policy defined. See “[Configuring Administrator Password Policy](#)” on page 34 in [Chapter 2](#) for more information

To change your Administrator password:

1. In the Administrative Console, click the **Change Password** link located in the Header frame.

The *Change Password* page appears.

2. Type the new **password** in the applicable fields and click **Submit**.

The system changes your password. The next time you log on to the Administrative Console, you will use this new password.

Updating Your Profile

Each administrator has a profile that specifies the preferred locale, number of records to be shown per report page as well as the default start date the system will initially choose in the report query pages. You may modify your profile as desired.

To update your profile:

1. In the Administrative Console, click the **Update Profile** link located in the Header frame.

The *Update Your Profile* page appears.

2. Type the **Records per page** and **Start date offset** information in the applicable fields. Select **Locale**, **Local Time Zone** and **Date Order for Report Generation** from the drop down menus and click **Submit**.

The following table provides information on the fields on the *Update Your Profile* page.

Table 1-4 Update Profile Page Fields

Field	Description
Records Per Page	The maximum number of records that the system will display on a report page. If you select --, Records Per Page defaults to a value set by the Issuer.
Start date offset	<p>The offset from the query date that the system will use by default. You can choose two different types of offsets:</p> <p>First day of the current month If chosen, by default the query range will start on the first day of the month and go through the day of the query.</p> <p>Number of days offset If you specify an integer value, the query range will start the specified number of days prior to the day of the query and go through the day of query.</p>

Table 1-4 Update Profile Page Fields

Field	Description
Locale	The preferred language of operation of the administrator. Select one of the languages from the drop-down menu.
Local Time Zone	The preferred time zone of the Issuer. This is the time zone used in reports.
Date Order for Report Generation	Display order for date input field for administrative reports. This parameter determines the input date format for search criterion used in administrative reports.

NOTE:

The administrator can set the locale from the drop-down menu in the header of the Administrative Console. This changes the locale only for that particular session. To set locale across sessions, change it using the *Update Your Profile* link.

The message “Admin Profile Updated Successfully” appears on the page.

Exporting a Report to a File

Every administrator report includes an option to export a report to a Comma Separated Value (CSV) file. You can then open these reports in another software application and manipulate the data as desired. This is the recommended method if any kind of post processing sorting is required for the reports.

To export a report to a file:

1. Click the desired report link.
The selected report page appears.
2. Type the report criteria in the applicable fields and click the **Export** button.
A *Save As* dialog box appears.
3. Select the directory in which to save the file, rename the file as desired, and click **Save**.

The system saves the file to the selected directory.

IMPORTANT:

Save the file as a .txt file instead of the default .csv extension. Follow the steps described below to ensure a successful export.

Viewing the Exported File

To view the exported file in Microsoft Excel:

1. Choose **File | Open**.

The *Open* dialog box appears.

2. Locate the .txt file you want to open, click on it to select it, and click **Open**.

The *Text Import Wizard* appears.

3. Click **Next** on the *Step 1 of 3* page without changing the default choices.

The *Step 2 of 3* page appears.

4. Under **Delimiters**, de-select **Tab**, select **Comma**, and then click **Next**.

The *Step 3 of 3* page appears.

5. Change the default data format for column(s) containing large numbers (for example, a PAN column) by selecting the particular column in the **Data preview** window and selecting **Text** under **Column data format**.

6. When you have completed the column data format changes, click **Finish**.

The report appears as an Excel spreadsheet.

Chapter 2

Managing Administrators

The Issuer Software administrative functions are distributed among four different groups of administrators. See “[Administrator Group Hierarchy](#)” on page 8 for more information regarding the groups and their relationship. This chapter discusses how to create and manage the administrators.

The chapter describes the following tasks needed to manage the administrators:

- [Creating Administrator Accounts](#)
- [Updating Administrator Privileges](#)
- [Enabling/Disabling Administrators](#)
- [Resetting Administrator Passwords](#)
- [Configuring Administrator Password Policy](#)
- [Configuring Administrator Privileges](#)
- [Master Administrator Operations](#)
- [Viewing Administrator System Access Reports](#)

NOTE:

This chapter describes all possible administrator related tasks. Whether you have the authority to complete the tasks described is defined by a higher level administrator.

NOTE:

With appropriate privileges, every group of administrators (except CSR's) can manage their own group and the next lower level administrator group.

Creating Administrator Accounts

Issuer Administrators are responsible for creating the Administrator (CSR) accounts and other Issuer Administrators for each Issuer.

Global Administrators are responsible for creating other Global Administrators. Master Administrators can also create Global Administrators. The following sections provide instructions on creating different type of administrator accounts:

NOTE:

Depending on your Issuer Administrator privileges configuration, some of these tasks may require dual control. See [“Dual Control” on page 15](#) for information on this concept.

Creating Administrators and Issuer Administrators

When you create an Administrator account, you define a User ID and temporary password for the Administrator. You can also adjust the default Administrator privileges for the particular Administrator.

To create CSR or Issuer Administrator accounts:

1. Click one of the following links:
 - For CSR accounts, choose the **Create Administrator** link.
 - For Issuer Administrator accounts, choose the **Create Issuer Administrator** link.

The appropriate page appears.

2. Select the applicable **Issuer**, type the desired **User ID** and **password** in the applicable fields.

NOTE:

The User ID must be a single character string. In other words, do not put a space in between words. Incorrect: M Smith. Correct: MSmith.

3. You can specify whether the Administrator must:
 - a. *Change Password at first login*

- b. Password never expires.*

You can select the check boxes provided for these options.

You can consider selecting the Password Never Expires option for administrators who are given Upload privileges.

4. If desired, select or clear any **Action and Report Privileges** to which you do not wish this Administrator to have access.
5. Click **Submit**.

The message “Admin Created Successfully” appears.

Creating Global Administrators

Global Administrators can be responsible for creating and managing other Global Administrator accounts. You can adjust the privileges for individual Global Administrator accounts based on the default privileges set for Global Administrators by your Master Administrators.

For information configuring Global Administrator privileges by a Master Administrator, see [“Configuring Administrator Privileges” on page 36](#).

When you create a Global Administrator account, you define a User ID and temporary password for the Global Administrator, as well as specifying the countries over which the Global Administrator will have control. You can also adjust the default Global Administrator privileges for the particular Global Administrator and define the list of Issuers the Global Administrator can support.

To create a Global Administrator account:

1. Click the **Create Global Admin** link.

The *Create Global Administrator* page appears.

2. Type the desired **User ID** and **password** in the applicable fields.
3. You can specify whether the Administrator must:
 - a. Change Password at first login*
 - b. Password never expires.*

You can select the check boxes provided for these options.

You can consider selecting the Password Never Expires option for administrators who are given Upload privileges.

4. To add a country over which the Global Administrator will have control, scroll through the **List of Countries** and select a **country**, then click >>>> to add the country to the **Selected Countries** box. To select multiple countries, press and hold **Ctrl** while selecting the desired countries and then click >>>>.

The **List of Countries** box only displays the countries over which you (and the other logged on Global Administrator, if dual control was enforced) have control.

To de-select a selected country, select the **country** in the **Selected Countries** box and click <<<<.

5. To add an Issuer over which the Global Administrator will have control, scroll through the **List of Issuers** and select an **Issuer**, then click >>>> to add the Issuer to the **Selected Issuers** box. To select multiple issuers, press and hold **Ctrl** while selecting the desired issuers and then click >>>>.

The **List of Issuers** box only displays the countries over which you (and the other logged on Global Administrator, if dual control was enforced) have control.

To de-select a selected issuer, select the **Issuer** in the **Selected Issuers** box and click <<<<.

6. If desired, de-select any **Action and Report Privileges** to which you do not wish this Global Administrator to have access.
7. Click **Submit**.

The message “Admin Created Successfully” appears.

Creating Global Administrators using the DUC

You can easily create and update Global Administrators using the Data Upload Client. This feature allows you to add or update a global administrator based on an existing model administrator. To add a new administrator the upload administrator uses the model admin to copy privileges, attributes and states to the new administrator and populates only specific unique requirements like userid and password. This utility improves productivity, ensures consistent definitions and ultimately reduces errors. See the *Arcot Data Upload Tool Installation and User Manual* for more details on how to use this feature.

The Master Administrator can create the Global administrator with the *Upload Admin Data* privilege. Global administrators having this privilege can create or update other global administrators using the DUC. They can also pass this privilege to the new administrators created.

Arcot recommends that you create the initial model administrator with necessary precautions. The new administrator created will have all the privileges, Issuer associations, state and any other attributes of the model administrator. If you update existing administrators, irrespective of whatever the current privileges, the administrators will get updated to the same attributes of the model administrator.

Arcot specifically recommends that you select the *Change password at first logon* option for the model administrator. The password policy is enforced on the newly created administrators. Arcot also strongly recommends that model administrator is not used to login to the console and perform any administrative operations. This will impact the state of the model administrator and any new administrators created or updated using DUC will get impacted. For example, at first login, the model administrator is asked to change password and this attribute is passed on to the other administrators created later.

Figure 2-1 Creating Model Global Administrator

Create Global Administrator

User ID, Password, select a list of countries for this administrator, check the appropriate privileges and it.

User ID: JohnSmith

Password: *****

Re-type Password: *****

☒ Admin must change password at first login

☐ Password Never Expires

List Of Countries

United Kingdom
United States
Uruguay
Uzbekistan

Selected Countries

United Kingdom
United States

List Of Issuers

Citibank
Citibank1
Citibank2
foram

Selected Issuers

Citibank

Updating Administrator Privileges

This function lets you adjust the privileges for an existing Administrator account.

Updating Administrator (CSR) and Issuer Administrator Privileges

To update Administrator privileges:

1. Click the **Update Administrator Privileges** link or the **Update Issuer Admin Privileges** link.

The *Update Issuer Administrator Privileges* or *Update Administrator Privileges* page appears.

2. Use the drop-down menu to select the desired Issuer.

A **User ID** field appears.

3. Use the drop-down menu to select the desired **User ID**.

The system displays a list of all possible **Action & Report Privileges** for an Administrator account.

4. Modify the privileges as desired.

5. Click **Submit**.

The message “Admin Profile Updated Successfully” appears.

This function lets you adjust the privileges for an existing Issuer Administrator account. The privileges correspond to menu links available to the Issuer Administrator.

Updating Global Administrator Privileges for a Selected Global Administrator

This function lets you adjust the privileges for an existing Global Administrator account. The privileges correspond to menu links available to the Global Administrator.

To update Global Administrator privileges:

1. Click the **Update Global Admin Privileges** link.

The *Update Global Administrator Privileges* page appears.

2. Use the drop-down menu to select the desired **User ID**.

The system displays a **List of Issuers** and a list of all possible **Action & Report Privileges** Global Administrator account.

3. Modify the list of issuers as desired.
4. Modify the privileges as desired.
5. Click **Submit**.

The message “Admin Profile Updated Successfully” appears.

Enabling/Disabling Administrators

There may be times when you need to disable an existing Administrator account (for example, an Administrator might be leaving the company or going on an extended leave of absence). Disabling an account locks that Administrator out of the system. Alternatively, there are times when you may need to enable a locked account (for example, when an Administrator returns from an extended leave of absence).

To enable or disable an Administrator account:

1. Click the appropriate link from the menu:
 - For Issuer Administrators choose, **Enable/Disable Issuer Admin Account**
 - For CSR's choose, **Enable/Disable Administrator Account**
 - For Global Administrators choose, **Enable/Disable Global Admin Account**

The appropriate page appears.

2. Use the drop-down menu to select the applicable **Issuer**.

The system displays a **User ID** field.

3. Use the drop-down menu to select the desired **User ID**.

The system displays the **Status** and **Remarks** fields.

4. Do one of the following:
 - a. To disable an Issuer Administrator, use the **Status** drop-down menu to select **Locked**.
 - b. To enable an Issuer Administrator, use the **Status** drop-down menu to select **Active**.
5. Type any **remarks** concerning the status change in the **Remarks** field.
6. Click **Submit**.

The message "Issuer Administrator Account Locked/Unlocked Successfully" appears.

Resetting Administrator Passwords

You can reset passwords for Administrators who forget their passwords. The new password should adhere to the password policy applicable to this Administrator. See [“Configuring Administrator Password Policy,”](#) for more information.

1. Click the appropriate link from the menu:
 - For Issuer Administrators choose, **Reset Issuer Admin Password.**
 - For CSR’s choose, **Reset Administrator Password**
 - For Global Administrators choose, **Reset Global Admin Password**

The appropriate page appears.

2. Use the drop-down menu to select the applicable **Issuer**.

The system displays a **User ID** field.

3. Use the drop-down menu to select the desired **User ID**.

The system displays the **New Password**, **Re-Type Password** and **Remarks** fields.

4. Type the **new password** and any **remarks** in the applicable fields and click **Submit**.

The message “Admin Password Modified Successfully” appears.

Configuring Administrator Password Policy

This function lets you configure password restrictions for the Administrators and Issuer Administrators accounts for a specific Issuer. The Master Administrator configures the password policy for all the Global administrators in the system. If you change this policy once it is in place, the new policy will only affect new Administrators or Administrators that change their passwords after the updated policy is in place. It will not affect the existing Administrator passwords.

To configure Administrator password policy:

1. Click the appropriate link from the menu:
 - For Issuer Administrators choose, **Configure Issuer Admin Policy**.
 - For CSR's choose, **Configure Administrator Policy**
 - For Global Administrators choose, **Configure Global Admin Policy**.

The appropriate page appears.

2. For the CSR's and Issuer Administrators, use the drop-down menu to select the desired **Issuer**.

The system displays the list of configurable password policy options.

3. Specify the desired values in the applicable fields.

The following table describes the Administrator password policy parameters. To disable a particular option, specify "--" in a drop-down list or leave a text field blank.

Table 2-1 Administrator Password Policy Parameters

Parameter	Description
Issuer	The Issuer to which these parameters will be applied.
Failed Login Attempts Allowed - Per Session	The number of times an incorrect login attempt may occur consecutively during a single session.
Failed Login Attempts Allowed - Across Sessions	The number of times an incorrect login attempt may occur consecutively across multiple sessions.
Password Length - Minimum	The minimum number of characters that a password must have to be valid.
Password Length - Maximum	The maximum number of characters that a password may have to be valid.

Table 2-1 Administrator Password Policy Parameters

Parameter	Description
Password Format Restriction - Minimum Numeric	The minimum number of numeric characters that must be used in the password.
Password Format Restriction - Minimum Alphabetics	The minimum number of alphabetic characters that must be used in the password.
Password Format Restriction- Minimum Special Characters	The minimum number of special characters that must be used in the cardholder's secret password. Special characters supported are: ! " # \$ % & ' () * + , - . / ; < = > ? @ .
Password Renewal frequency	The maximum number of days that a password will remain valid before it must be changed.
Maximum Inactivity Period	The maximum number of days that an account may be inactive before the account is suspended.
Allow admin to reset password after expiry	If you select this check box, you can allow the administrators to reset their password after a lockout due to password expiration or administrator inactivity.

4. When you have completed your modifications, click **Submit**.

The message “Admin Configuration Params Updated Successfully” appears.

Configuring Administrator Privileges

This function lets you define a default set of privileges to use for all Administrators. The privileges correspond to the menu links that are displayed for the Administrator accounts.

NOTE:

Only a Global Administrator can configure the privileges of all the CSRs and Issuer Administrators. The Master Administrators can configure the privileges for all the Global administrators in the system.

To configure Administrator privileges:

1. Click the appropriate link from the menu:
 - For Issuer Administrators choose, **Configure Issuer Admin Privileges**.
 - For CSR's choose, **Configure Administrator Privileges**
 - For Global Administrators choose, **Configure Global Administrator Privileges**.

The appropriate page appears. This page lists all of the possible Administrator menu options and indicates whether the option is a report or an action and whether the option requires dual control.

2. Use the **Enable** check box to specify an option as enabled and the **Dual Control** check box to specify an option as requiring dual control.

See **“Dual Control” on page 15** for information on the dual control concept.

3. When you have completed configuring the privileges, click **Submit**.

The message “Admin Privileges Updated Successfully” appears.

Master Administrator Operations

When the Issuer Software is installed, the installation process creates two Master Administrator accounts. There will only be two Master Administrator accounts per Issuer Software deployment.

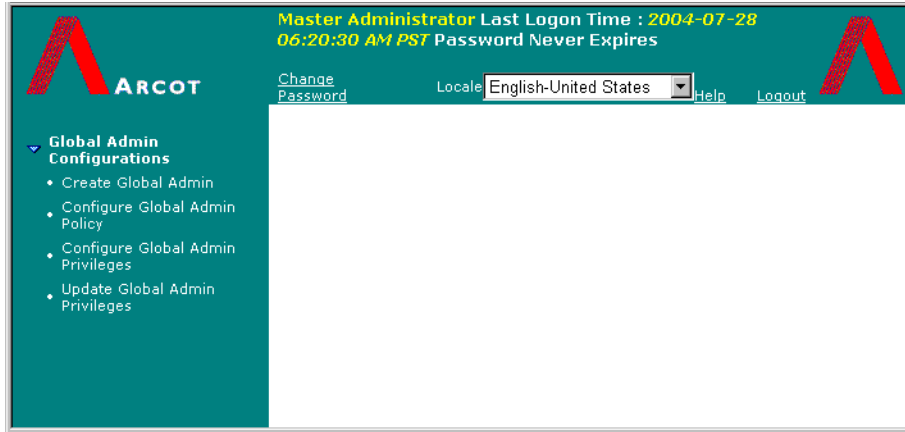
The primary responsibility of the Master Administrators is to create Global Administrator accounts and define the Global Administrator account access privileges. This section provides instructions for the tasks related to managing Global Administrator accounts.

Managing Global Administrator Accounts

Both Master Administrators must be present and enter their separate passwords before they can perform any Global Administrator account management tasks. See [“Logging in and out of the Administrative Console” on page 19](#) for detailed instructions on Master Administrator login.

Master Administrators can perform the following tasks:

- Create Global Administrator accounts. See [“Creating Global Administrators,”](#) for detailed instructions.
- Configure Global Administrator password policy. See [“Configuring Administrator Password Policy,”](#) for detailed instructions.
- Configure Global Administrator privileges. See [“Configuring Administrator Privileges,”](#) for detailed instructions.
- Update Global Administrator privileges. See [“Updating Administrator Privileges,”](#) for detailed instructions.

Figure 2-2 Master Administrator Page

Viewing Administrator System Access Reports

All the administrator access to the Issuer Software system are recorded in two types of logs:

- Activities Log
- Report Access Log

The Issuer Administrator can view these reports to retrieve and display information about Administrators (CSRs) and Issuer Administrators system use. The Global Administrator can view the system access reports for CSRs, Issuer Administrators and Global Administrators.

You can choose to view a report online or export a report to a file to use in another software program.

NOTE:

This section provides instructions on how to view reports online. See [“Exporting a Report to a File” on page 22](#) for instructions on how to export a report.

The system displays reports according to the information set up in your Report Profile. See the [“Updating Your Profile” on page 21](#) for information on how to change your Report Profile.

The reports according to the administration level fall into the following categories:

- [CSR System Access Reports](#)
- [Issuer Administrator Account Reports](#)
- Global Administrator Account Reports

This section describes the information contained in each report and provides instructions on how to access and view each report.

CSR System Access Reports

There are two reports that display information about Administrator (CSR) system access:

- [Administrator Report Access Log](#)
- [Administrator Activities Log](#)

Administrator Report Access Log

The Administrator Report Access Log displays the report access activities performed by Administrators (CSRs) in a given time period. This report displays the following information:

Table 2-2 Administrator Report Access Log fields

Report Field	Description
Issuer Name	The name of the Issuer.
Admin Name	The Administrator's User ID.
Report Type	The name of the report that the corresponding Administrator ran.
Card Number	The card number the Administrator defined when running the corresponding report (not applicable to all reports).
Start Date	The start date of the date range defined by the Administrator when running the report.
End Date	The end date of the date range defined by the Administrator when running the report.
Date Accessed	The date the Administrator ran the report.

To view the Administrator Report Access Log:

1. Click the **Administrator Report Access Log** link.

The *Administrator Report Access* page appears.

2. Select **All Admins** or a specific **User ID**, type the desired **From/To date range**, and click **Submit**.

The system displays the report.

Administrator Activities Log

The Administrator Activities Log displays information regarding the system activities performed by Administrators in a given time period. This report displays the following information:

Table 2-3 Administrator Activities Log fields

Report Field	Description
Issuer Name	The name of the Issuer.
Admin Name	The Administrator's User ID.
Action	The task performed by the Administrator (for example, Cardholder Account Enquiry)

Table 2-3 Administrator Activities Log fields

Report Field	Description
Cardholder Name	The name of the cardholder associated with the corresponding Action (not applicable to all actions).
Card Number	The card number associated with the corresponding Action (not applicable to all actions).
Date Accessed	The date the action was performed.
Detail	Any system information regarding the action (for example, Admin Logged in Successfully).

To view the Administrator Activities Log:

1. Click the **Administrator Activities Log** link.

The *Administrator Activities Log* page appears.

2. Select **All Admins** or a specific **User ID**, type the desired **From/To date range**, and click **Submit**.

The system displays the report.

Issuer Administrator Account Reports

There are two reports that display information about Issuer Administrator system access:

- [Issuer Administrator Report Access Log](#)
- [Issuer Administrator Activities Log Report](#)

Issuer Administrator Report Access Log

The Issuer Administrator Report Access Log displays the report access activities performed by Issuer Administrators in a given time period.

See [Table 2-2 on page 40](#) for descriptions of the information displayed by this report.

To view the Issuer Administrator Report Access Log:

1. Click the **Issuer Admin Report Access Log** link.

The *Issuer Admin Report Access Log* page appears.

2. Select **All Admins** or a specific **User ID**, type the desired **From/To date range**, and click **Submit**.

The system displays the report.

Issuer Administrator Activities Log Report

The Issuer Administrator Activities Log displays information regarding the system activities performed by Administrators in a given time period. The report displays the following information:

Table 2-4 Issuer Administrator Activities Log Report

Report Field	Description
Issuer Name	The name of the Issuer
Admin Name	The Issuer Administrator's User ID.
Action	The task performed by the Issuer Administrator (for example, Admin Login).
Date Accessed	The date the task was performed.
Detail	Any system information regarding the action (for example, Admin Logged in Successfully).

To view the Issuer Administrator Activities Log:

1. Click the **Issuer Admin Activities Log** link.

The *Issuer Admin Activities Log* page appears.

2. Select **All Admins** or a specific **User ID**, type the desired **From/To date range**, and click **Submit**.

The system displays the report.

Global Administrator Account Reports

Global Administrator Activities Log

The Global Administrator Activities Log displays information regarding the system activities performed by Global Administrators in a given time period. This report displays the following information:

Table 2-5 Global Administrator Activities Log fields

Report Field	Description
Admin Name	The Global Administrator's User ID.
Action	The task performed by the corresponding Global Administrator. (For example, Update FI Information)
Date Accessed	The date the action was performed.

Table 2-5 Global Administrator Activities Log fields

Report Field	Description
Detail	Upon being expanded, displays the details associated with the corresponding Action (for example, parameters changed, messages displayed, and so on).

To view the Global Administrator Activities Log:

1. Click the **Global Admin Activities Log** link.

The *Global Administrator Activities Log* page appears.

2. Select **All Admins** or a specific **User ID**, type the desired **From/To date range**, and click **Submit**.

The system displays the report.

Global Administrator Report Access Log

The Global Administrator Report Access Log displays the report access activities performed by Global Administrators in a given time period.

See following table for descriptions of the information displayed by this report.

Table 2-6 Global Administrator Activities Log Report

Report Field	Description
Admin Name	The Global Administrator's User ID.
Report Type	The name of the report that the corresponding Administrator ran.
Start Date	The start date of the date range defined by the Administrator when running the report.
End Date	The end date of the date range defined by the Administrator when running the report.
Date Accessed	The date the Administrator ran the report.

To view the Global Administrator Report Access Log:

1. Click the **Global Admin Report Access Log** link.

The *Global Admin Report Access Log* page appears.

2. Select **All Admins** or a specific **User ID**, type the desired **From/To date range**, and click **Submit**.

The system displays the report.

Figure 2-3 Report Access Log

Global Admin Report Access Log

AS OF DATE:2001-10-04 -- 2004-06-29

Run date/time:2004-06-29 11:27:51 PM PST

1

Retrieved:77 Displaying:1 - 77

Admin Name	Report Type	Start Date	End Date	Date Accessed
VGA	GLOBAL_ADMIN_ACTIVITIES_LOG	2001-10-04 12:00:00 AM PST	2004-06-29 11:59:59 PM PST	2004-06-29 11:28:44 PM PST
VGA	SUCCESSFUL_REGISTRATIONS	2001-10-02 12:00:00 AM PST	2004-06-27 11:59:59 PM PST	2004-06-27 11:33:03 PM PST
VGA	SUCCESSFUL_REGISTRATIONS	2001-10-02 12:00:00 AM PST	2004-06-27 11:59:59 PM PST	2004-06-27 11:32:35 PM PST
VGA	SUCCESSFUL_REGISTRATIONS	2001-10-02 12:00:00 AM PST	2004-06-27 11:59:59 PM PST	2004-06-27 11:32:23 PM PST
VGA	SUCCESSFUL_REGISTRATIONS	2001-10-02 12:00:00 AM PST	2004-06-27 11:59:59 PM PST	2004-06-27 11:31:38 PM PST
VGA	SUCCESSFUL_REGISTRATIONS	2001-09-28 12:00:00 AM PST	2004-06-23 11:59:59 PM PST	2004-06-23 04:10:10 AM PST

Figure 2-4 Activities Log

Global Administrator Activities Log

AS OF DATE:2001-10-04 -- 2004-06-29Run date/time:2004-06-29 11:30:56 PM PST

1 2 3 4 5 [Next>>]

Retrieved:404 Displaying:1 - 100

Admin Name	Action	Date Accessed	Detail
VGA	Admin Login	2004-06-29 11:32:38 PM PST	Detail
VGA	Admin Login	2004-06-29 11:32:30 PM PST	Detail
VGA	Admin Login	2004-06-29 11:28:28 PM PST	Detail
VGA	Update FI Information	2004-06-29 10:31:57 PM PST	Detail
VGA	Update FI Information	2004-06-29 10:31:41 PM PST	Detail

Figure 2-5 Activity Details

Global Administrator Activities Log	
AS OF DATE: 2001-10-04 -- 2004-06-29 Run date/time: 2004-06-29 11:32:13 PM PST	
Admin Name	VGA
Action	Admin Login
Date Accessed	2004-06-29 11:32:38 PM PST
Column/Parameter Name	Value
Message	Primary Admin has got privilege from a peer Admin

Administrator (CSR) Operations

Your Issuer's cardholders will contact your applicable customer service department with a variety of service needs related to 3-D Secure enrollment and their secret passwords. For example, cardholders may have difficulty completing a 3-D Secure enrollment, cardholders may forget their secret passwords or want to change their passwords for security reasons, and so on.

This chapter describes the following topics related to managing cardholder enrollment:

- Standard, Abridged and Activation During Shopping (ADS)
- Managing Cardholder Accounts

NOTE:

This chapter describes all possible Administrator privileges. Whether or not you have authority to complete the tasks described is defined by your Issuer Administrator.

About Cardholder Enrollment

This section describes the following cardholder enrollment processes:

- [Standard Enrollment](#)
- [Abridged Enrollment](#)
- [Activation During Shopping \(ADS\)](#)

Standard Enrollment

Many cardholders will enroll in the 3-D Secure program using their Issuer's enrollment Web site. This Web site is part of the Issuer Software and operates without any interaction with the Issuer's Administrators (CSR). This section describes the cardholder's interaction with the system.

There are two steps involved in a standard enrollment:

- [Verifying Cardholder Identity](#)
- [Creating the Cardholder's Identifiers](#)

Verifying Cardholder Identity

The first step in a standard enrollment is verifying the identity of the cardholder that is attempting to enroll in the 3-D Secure program. The Issuer determines its own method of verifying the cardholder. See the *Arcot TransFort Issuer Software Introduction Manual* for detailed information about these verification methods.

During the verification process, the cardholder answers a set of questions related to the cardholder's identity (personal information such as credit card billing address, mother's maiden name, and so on), and about the cardholder's credit history and financial activities. The responses to these questions are verified based on the verification method employed.

Creating the Cardholder's Identifiers

Once the cardholder's identity has been established, the system prompts the cardholder to create a secret password. The cardholder will use this password for all 3-D Secure purchase transactions at participating merchant Web sites.

Next, the cardholder creates a personal message. This message is displayed any time the cardholder makes an online purchase using the 3-D Secure program. This message appears during a purchase transaction and offers the cardholder assurance that the transaction is secure and valid.

The cardholder may also be prompted to create a hint and response, depending on the Issuer cardholder enrollment configuration. The response to the hint acts as a secondary password to identify the cardholder in the event that the cardholder forgets the secret password.

Once the cardholder has been successfully enrolled, the cardholder is free to make purchases on participating merchant Web sites.

Abridged Enrollment

In certain cases, it may be appropriate for you to manually enroll some of your cardholders. This is called an **Abridged Enrollment**, and basically consists of you adding the cardholder's name and card number to the Issuer Software database and giving the cardholder a temporary password to use at your Issuer's Abridged Enrollment Web site. If you manually enroll a cardholder, the cardholder does not have to perform the standard enrollment process and is allowed to perform only a small subset of the steps required to enroll in the 3-D Secure program.

An Abridged Enrollment may be appropriate for cardholders who have had difficulty completing the standard enrollment process. You may also choose to use Abridged Enrollments for your preferred customers (VIPs).

NOTE:

Cardholder identity verification is not enabled in the system for Abridged Enrollments. It is the Issuer's responsibility to verify the identity of cardholder's requesting Abridged Enrollment. For information on your company's policies regarding Abridged Enrollment, see your manager.

For information on how to manually enroll a cardholder, see [“Adding Cardholder Accounts” on page 49](#).

Activation During Shopping (ADS)

An Issuer can automatically enroll cardholders into the online payer authentication program. Issuers can enable ADS in three ways:

1. **Opt-In**
2. **Issuer Activation**

3. Purchase Attempts

These features are described in the section below.

Opt-In

In this method the cardholder is introduced to the online payer authentication program while purchasing at a participating merchant's web site. The cardholder is presented with an opt-in page which may include a temporary password hint. If the cardholder chooses to enroll at this point the password page appears and the purchase transaction continues as a authenticated transaction and the cardholder is auto-enrolled into the program. The cardholder has a choice of opt-in later and the purchase transaction is still completed in this case, but as a non-authenticated transaction. The opt-in page is shown again when the cardholder makes purchases and the number of times this page appears is decided by the Issuer.

Issuer Activation

The cardholder can be forced to enroll into the program by showing the welcome page directly. Also, if the cardholder defers the OptIn feature for a maximum number of times, the number being decided by the Issuer, the Issuer can enforce enrollment of the cardholder. This enrollment is communicated the next time the cardholder attempts a purchase transaction. The cardholder is welcomed into the online payer authentication program and the password page appears. At this point the cardholder is forced to enter the password to complete the transaction. On completing this step, the cardholder the auto enrolled into the program.

Purchase Attempts

The cardholder configured for the Attempts feature is introduced to the virtues of the online payer authentication program. The cardholder information is logged in the Issuer Software Database and the purchase continues as a non-authenticated transaction. This information can be used to spotlight active shoppers over the internet. Such cardholders can be potential candidates for the online payer authentication program. The statistical information can be used as a marketing/sales tool.

You can see the *Arcot TransFort Issuer Software Introduction Manual* for more information about the end user experience during ADS.

Managing Cardholder Accounts

This section provides detailed instructions on how to use the Administrative Console to perform the following cardholder account tasks:

- [Adding Cardholder Accounts](#)
- [Viewing Cardholder Account Information](#)
- [Updating the User ID](#)
- [Locking/Unlocking Cardholder Accounts](#)
- [Viewing the details of a particular cardholder's account](#)
- [Updating Cardholder Enrollment Responses](#)
- [Resetting a Cardholder's Password](#)
- [Cancelling Cardholder Accounts](#)
- [Receiving Promotional Emails](#)
- [View/update Do Not Prompt](#)
- [Changing the Locale of a Card](#)

NOTE:

The procedures in this section assume you are already logged on to the Administrative Console as an Administrator. See [“Logging in and out of the Administrative Console”](#) on page 19 for detailed instructions.

Adding Cardholder Accounts

This function allows you to enroll a cardholder using the [Abridged Enrollment](#) method. To manually enroll a cardholder, complete the required information in the *Add Cardholder* page. Then give the cardholder a temporary password and the URL to your Issuer's Abridged Enrollment Web site. The cardholder will then complete a subset of the enrollment process on this Web site.

The temporary password that you give the cardholder expires after a designated amount of time. For example, your company may require that the cardholder access the Abridged Enrollment Web site and enroll within 48 hours of talking to the Administrator (CSR). This temporary password time limit is configurable, and is set by the Issuer Administrator. For information about configuring temporary password duration, see [“Configuring Issuer Parameters”](#) in [Chapter 4](#).

CAUTION:

Before adding a cardholder using the Abridged Enrollment method, ensure that you know and understand your company's policies regarding this type of enrollment.

To add a cardholder account:

1. Click the **Add Cardholder** link.

The *Add Cardholder* page appears.

2. Enter the card number and click **Submit**.

The page asks for more information.

3. Enter the applicable information in the appropriate fields.

The following table provides detailed descriptions of each field.

Table 3-1 Add Cardholder Fields

Field	Description
Name	The name of the cardholder as it appears on the card.
Password	<p>The temporary password that the cardholder will use to log on to the Abridged Enrollment Web site to complete the enrollment process.</p> <p>You can choose to either enter a password or click the provided link to have the system generate a random password.</p>
Reason	<p>The reason that the cardholder is being manually enrolled. There are two options:</p> <p>Failed User User was unable to complete the standard registration.</p> <p>VIP Registered due to the customer's preferred cardholder status.</p>
Remarks	Additional information regarding the need to perform an Abridged Enrollment for the cardholder or how the cardholder identity was verified.

4. Click **Submit**.

The message "Cardholder <name> added" appears.

Remember to give the temporary password, password duration, and Abridged Enrollment Web site URL to the cardholder once you add the account. If you do not know the default password duration or URL, contact your supervisor.

NOTE:

An Issuer can configure the cardholder enrollment parameters making only the card number mandatory for enrollment. The cardholder name could be an optional field. If you are using such a configuration, leave the Name field empty, and enter only the card number and the temporary password.

NOTE:

You will be unable to view the cardholder you just added in any other tasks or report options except the Cardholders Added by Administrator report until the cardholder completes the enrollment process on your Abridged Enrollment Web site.

Viewing Cardholder Account Information

The Cardholder Account Inquiry function allows you to view the account information of a particular cardholder. This function also provides links to the following cardholder account functions:

- Update the cardholder responses to Issuer questions
- Reset the cardholder's secret password.
- Update The cardholder's User ID
- Cancel the cardholder's 3-D Secure Service
- To allow the cardholder to receive Promotional Emails
- View/Update Do Not Prompt for a cardholder
- To lock/unlock the cardholder from the 3-D Secure Service
- Viewing the details of a particular cardholder's account.
- Changing the locale of a card.

NOTE:

You will be unable to use this function to view information for cardholders who have been added to the system using the Abridged Enrollment process but have not completed the enrollment. To view information for such cardholders, see the *Arcot TransFort Issuer Software Reports Manual*.

1. Click the **Cardholder Account Inquiry** link.

The *Cardholder Account Inquiry* page appears.

2. Type the **card number** in the applicable field and click **Submit**.

The system displays the account information for the selected card number in three tables:

- Enrolled Cardholders - Activated and Pre-Activated
- Pre Enrolled Cardholders
- Cancelled Cardholders

The following tables provides detailed information of the fields in each of the displayed cardholder tables:

Table 3-2 Enrolled Cardholders

Field	Description
Cardholder Name	The name of the cardholder as it appears on the card. This is a link which provides details of the particular cardholder. It also displays the last three 3-D Secure purchase transactions authenticated for the selected cardholder.
Update User ID	This link allows the administrator to update the cardholder's User ID provided he has the privilege to "Reset Password" for the cardholders.
Expiration Date	The expiration date of the card.
	WARNING This field might not contain a valid value always. It might include the unused constant "2100/12" for cardholders that have enrolled through ADS.
Enabled	This check box indicates if the enrolled card is enabled for the 3-D Secure program.
Reset Cardholder Password	This link allows the administrator to reset the cardholder's secret password. You can reset the passwords of only the Activated cardholders.
Update Cardholder Registration Data	This link allows the administrator to update the cardholders answers to the Issuer's questions.
Cancel 3-D Secure Service	This check box allows the administrator to deactivate the cardholder from the 3-D Secure program.
Receive Promotional Emails	This checkbox is to indicate if the cardholder wants to receive promotional e-mails. The administrator can update this provided he has "Lock/Unlock" cardholder privilege.

Table 3-2 Enrolled Cardholders

Field	Description
Status	<p>This column displays the status of the cardholder. The possible values are:</p> <ul style="list-style-type: none"> • Activated - which means that the cardholder is enrolled and can perform an authenticated transaction. • Not yet Activated - which means the cardholder is enrolled, but has to complete validation and 'Activate' the account before attempting an authenticated transaction.
Callout Data	This column is populated by callouts. You can display any relevant information passed by the callouts.
Do Not Prompt	The administrator can view/update this option provided he has the privilege to "Cancel Enrollment" for the cardholders.

Table 3-3 Pre Enrolled Cardholders

Field	Description
Cardholder Name	The name of the cardholder as it appears on the card.
Update Cardholder Registration Data	This link allows the administrator to update the pre-enrolled cardholders answers to the Issuer's questions.

Table 3-4 Cancelled Cardholders

Field	Description
Cardholder Name	The name of the cardholder as it appears on the card. This is a link which provides details of the particular cardholder.
Expiration Date	The expiration date of the card you are enrolling.

3. The page displays a **Locale** drop-down box to select any of the Issuer supported locales for the card. The locale is changed for all the cardholders for the card.

The page also displays a **Remarks** text box where the administrator can enter any remarks for the actions performed. You can also choose a **Reason** for cancelling the 3-D Secure service from the drop down box.

Figure 3-1 Cardholder Account Inquiry Page

Cardholder Account Inquiry

This option allows you to make cardholder account enquiry, activate/deactivate a cardholder, reset cardholder's password, update cardholder registration data, cancel "3-D Secure" service and also update User ID if supported.

Card Number: 1000100010001002 Select locale: English-United States ▼

Enrolled Cardholders									
Card Holder Name	Update User ID	Expiration Date	Enabled	Reset Cardholder Password	Update Cardholder Registration Data	Cancel 3-D Secure Service	Receive Promotional Emails	Status	Callout Data
JOHN SMITH	JOHN SMITH		✓	Reset	Update	<input type="checkbox"/>	<input type="checkbox"/>	Activated	null
ANN SMITH	ANN SMITH		✓	Reset	Update	<input type="checkbox"/>	<input type="checkbox"/>	Activated	null

Do Not Prompt: ☐

Reason for cancelling 3-D secure service: Lost/Stolen ▼

Remarks:

Submit
Cancel

Updating the User ID

When a cardholder forgets the User ID or for other security reasons wants to change the User ID, you can update the User ID for the cardholder.

To update cardholder's User ID:

1. Click the **Cardholder Account Inquiry** link. Type the card number in the applicable field and click **Submit**.
2. The system displays the account information for the selected card number in the *Enrolled Cardholders* table.
3. In the **Update UserID** field click on the User Id that you want to change to display *Update User ID* page.
4. Enter a new User ID in the **New User ID** field and click **Submit**.

Locking/Unlocking Cardholder Accounts

When required you can lock or unlock a cardholder account. Locking a cardholder's account temporarily prevents the cardholder from doing 3-D Secure transactions.

To lock/unlock a cardholder account:

1. Click the **Cardholder Account Inquiry** link.
The *Cardholder Account Inquiry* page appears.
2. Type the **card number** in the applicable field and click **Submit**.
The system displays the account information for the selected card number.
3. Do one of the following:
 - a. To lock a cardholder account, clear the **Enabled** check box.
 - b. To unlock a cardholder account, select the **Enabled** check box.
You can add any appropriate remarks in the text box provided.
4. Click **Submit**. The system displays the *Cardholder Account Inquiry* page with the message "Locked/unlocked cardholder account successfully."

Viewing the details of a particular cardholder's account

1. Click the **Cardholder Account Inquiry** link.
The *Cardholder Account Inquiry* page appears.
2. Type the **card number** in the applicable field and click **Submit**.
The system displays the account information for the selected card number.
3. To view the details of the selected cardholder account, click on the **cardholder name** in the appropriate section.

The system displays the following details for the cardholder:

- Card Number
- Cardholder Name
- Enabled - a yes/no display to indicated whether cardholder is locked or unlocked

- Enrollment Date
- Date Activated - a timestamp when the cardholder is validated and the status is changed from pre-activated to activated.
- All successful 3-D Secure transactions
- Date on which the 3-D Secure service was cancelled (if cancelled)
- Date on which any cardholder information was updated by the cardholder using the Account Assistant.

NOTE:

This field is updated when a CSR updates the account information or when a cardholder updates account information using the *Update Your Profile* link on the enrollment website.

Updating Cardholder Enrollment Responses

When cardholders enroll in the 3-D Secure program, they may respond to one or more questions regarding their identity, depending on how the Issuer Enrollment site is configured. If requested to do so by a cardholder, you can update the cardholder's responses to these questions. You can update the responses of both enrolled cardholders and pre enrolled cardholders.

To update cardholder's responses:

1. Click the **Cardholder Account Inquiry** link.

The *Cardholder Account Inquiry* page appears.

2. Type the **card number** in the applicable field and click **Submit**.

The system displays the account information for the selected card number.

NOTE:

The card number you have entered is displayed in the top left corner of the account information table.

3. Do any one of the following
 - a. Click the **Update** link in the *Enrolled Cardholders* table to update the responses of the particular enrolled cardholder.

- b. Click the **Update** link in the *Pre Enrolled Cardholders* table to update the responses of the particular pre enrolled cardholder

The *Modify Cardholder Responses to Issuer's Questions* page appears. The page displays the card number, cardholder name, the Issuer's questions, and cardholder's responses.

4. Modify the responses, update the **Remarks** field, and click **Submit**.

The system displays the *Cardholder Account Inquiry* Page with the message "Issuer answers have been updated successfully".

Resetting a Cardholder's Password

When a cardholder forgets the secret password or for other security reasons wants to change the secret password, you can create a temporary password for the cardholder. The cardholder can then use the temporary password to change the secret password via the *Forgot your password?* link on the Issuer's Enrollment Web site.

1. Click the **Cardholder Account Inquiry** link.

The *Cardholder Account Inquiry* page appears.

2. Type the **card number** in the applicable field and click **Submit**.

The system displays the account information for the selected card number.

3. Click the **Reset** link for the particular cardholder in the *Enrolled Cardholders* table.

The *Reset Cardholder Password* page appears and displays the cardholder's name, card number, and card expiration date.

4. Type the **new password** and any **remarks** in the applicable fields.

If you want the system to randomly generate a password, click the **Click here to generate a password** link instead of typing anything in the **Password** field. The system generates a password and populates the **Password** field.

5. Click **Submit**.

The system displays the *Cardholder Account Inquiry* Page with the message "Temporary password created for cardholder <name>" appears. Give the temporary password, password duration, and URL to the 'Forgot your Password?' or 'Reset Password' on the Enrollment Web Site to the cardholder and tell the cardholder to change the password before it expires.

Cancelling Cardholder Accounts

Cancelling a cardholder account removes the 3-D Secure service from the cardholder's account. It does *not* cancel the actual credit card account.

1. Click the **Cardholder Account Inquiry** link.

The *Cardholder Account Inquiry* page appears.

2. Type the **card number** in the applicable field and click **Submit**.

The system displays the account information for the selected card number.

3. Select the check box of the **cardholder name(s)** you wish to deactivate and click **Submit**. You can choose a reason for cancelling from the drop-down box provided.

The system displays the *Cardholder Account Inquiry* Page with the message "Cardholder <name> deactivated". The *Cancelled Cardholders* table on the page is updated with this information. Clicking on the cardholder name will display the details of that particular account.

Receiving Promotional Emails

1. Click the **Cardholder Account Inquiry** link.

The *Cardholder Account Inquiry* page appears.

2. Type the **card number** in the applicable field and click **Submit**.

The system displays the account information for the selected card number.

3. Select the check box of the **cardholder name(s)** who wish to receive promotional Emails and click **Submit**.

View/update Do Not Prompt

1. Click the **Cardholder Account Inquiry** link.

The *Cardholder Account Inquiry* page appears.

2. Type the **card number** in the applicable field and click **Submit**.

The system displays the account information for the selected card number.

3. Select the Do Not Prompt check box to indicate that no prompts will be received by the cardholder(s) and click **Submit**.

Changing the Locale of a Card

You can choose the locale of the card from the list of locales which the Issuer supports. This locale becomes the preferred locale for all the cardholders for the given card number. The cardholder can view the CAP pages in this locale.

1. Click the **Cardholder Account Inquiry** link.

The *Cardholder Account Inquiry* page appears.

2. Type the **card number** in the applicable field and click **Submit**.

The system displays the account information for the selected card number.

3. Select the preferred locale you want from the drop-down box provided. This is the total list of locales supported by the Issuer.

Click **Submit**. The system displays a message “Locale Changed Successfully”.

Issuer Administrator Operations

Issuer Administrators are responsible for configuring the Issuer accounts in regards to cardholder enrollment in the 3-D Secure program. Issuer accounts are created by Global Administrators. For information on creating Issuer accounts, see “[Setting Up Issuer Accounts](#)” in [Chapter 5](#).

NOTE:

This tasks described in this chapter are privileges of an Issuer Administrator. Whether or not you have authority to complete the tasks described is defined by another Issuer Administrator or your Global Administrator.

This section provides instructions on the following tasks relating to Issuer accounts:

- Configuring Issuer Parameters
- Managing Administrators and Issuer Administrators

NOTE:

The procedures in the following sections assume you are already logged on to the Administrative Console as an Issuer Administrator. See “[Logging in and out of the Administrative Console](#)” on [page 19](#) for detailed instructions.

Configuring Issuer Parameters

As an Issuer Administrator, you can configure certain parameters that affect how the Issuer Enrollment Web site performs certain functions and how the Administrative Console is displayed. You can also define the password policy for the Issuer's cardholders.

To configure Issuer parameters:

1. Click the **Configure Issuer Parameters** link.

The *Issuer Configuration Parameters* page appears.

Figure 4-1 Configure Issuer Parameters Screen

Issuer Configuration Parameters	
Configure the appropriate values for the Issuer configuration parameters and click Submit .	
Default Report Display Parameters for Admin	
Date Order for Report Generation	Month, Day and Year ▾
Time Stamp Format in Report	yyyy-MM-dd hh:mm:ss a z ▾
Records Per Page	20 ▾
Admin Display Parameters	
Link to Arcot Home	Yes ▾
Display Arcot Symbol	Yes ▾
Data Upload Parameters	
DU Passphrase	****
Re-type DU Passphrase	****
Cardholder Display Parameters (ACS-CAP)	
Date Format	YY:DD:MM ▾
Date Separator	: ▾
Cardholder Authentication Parameters	
Temp Password Duration	4
Action for Cardholder Authentication after failed login attempts	
Lock Account	<input checked="" type="checkbox"/>
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

2. The following table provides descriptions of the Issuer parameters:

Table 4-1 Issuer Parameters

Parameter	Description
Default Report Display Parameters for Administrative Console	
Date Order for Report Generation	<p>The date order to be used during report generation.</p> <p>The following formats are available:</p> <p>Month, Day and year</p> <p>Year, Month and Day</p> <p>Day, Month and Year</p>
Time Stamp Format in Report	<p>The timestamps format that will be used in system reports.</p> <p>The following formats are available (examples of each shown):</p> <p>yyyy-MM-dd hh:mm:ss a z 2002-08-28 10:38:10 PM GMT</p> <p>MM-dd-yyyy hh:mm:ss a z 08-28-2002 10:38:10 PM GMT</p> <p>MM/dd/yyyy hh:mm:ss a z 08/28/2002 10:38:10 PM GMT</p>
Records Per Page	The default number of records that the system will display on administrator reports.
Administrative Console Display Parameters:	
Display Arcot Symbol	Whether or not the Arcot Systems logo will appear in the Administrative Console.
Link to Arcot Home	<p>Whether or not the Arcot Systems logo is linked to the Arcot Systems home page.</p> <p>This feature is not valid if the Display Arcot Symbol parameter is disabled.</p>
Data Upload Parameters:	
DU Pass Phrase	The passphrase used by the Upload Encryption Tool of the Data Upload Tool to encrypt the Issuer's data during upload. See <i>Arcot Data Upload Tool for Transfort Installation and User Manual</i> for more information.
Cardholder Display Parameters:	

Table 4-1 Issuer Parameters

Parameter	Description																
Date Format	<p>The format that will be used to display the date during purchase transactions. The following date formats are available (examples of each shown):</p> <table> <tr> <td>MM:DD:YY</td><td>08:28:02</td></tr> <tr> <td>DD:MM:YY</td><td>28:08:02</td></tr> <tr> <td>YY:MM:DD</td><td>02:08:28</td></tr> <tr> <td>YY:DD:MM</td><td>02:28:08</td></tr> <tr> <td>MM:DD:YYYY</td><td>08:28:2002</td></tr> <tr> <td>DD:MM:YYYY</td><td>28:08:2002</td></tr> <tr> <td>YYYY:MM:DD</td><td>2002:08:28</td></tr> <tr> <td>YYYY:DD:MM</td><td>2002:28:08</td></tr> </table>	MM:DD:YY	08:28:02	DD:MM:YY	28:08:02	YY:MM:DD	02:08:28	YY:DD:MM	02:28:08	MM:DD:YYYY	08:28:2002	DD:MM:YYYY	28:08:2002	YYYY:MM:DD	2002:08:28	YYYY:DD:MM	2002:28:08
MM:DD:YY	08:28:02																
DD:MM:YY	28:08:02																
YY:MM:DD	02:08:28																
YY:DD:MM	02:28:08																
MM:DD:YYYY	08:28:2002																
DD:MM:YYYY	28:08:2002																
YYYY:MM:DD	2002:08:28																
YYYY:DD:MM	2002:28:08																
Date Separator	<p>Specifies the type of separator that will be used to separate the different elements of the date. The following date formats are available:</p> <p>:</p> <p>/</p> <p>-</p> <p>.</p>																
Cardholder Authentication Parameters:																	
Temp Password Duration	The temporary password duration for the cardholder enrolling through “ Abridged Enrollment ,” is configured here. This field configures the number of days for which cardholder's temporary password is effective.																
Action for Authentication after failed login attempts	This set of responses specifies how the system reacts to failed login attempts. The Global Administrator specifies the number of login attempts that can be made unsuccessfully. See “ Adding Financial Institution Information to the Issuer Account ” for information on configuring the maximum number of authentication tries.																
Lock Password	Indicates whether or not the system should lock the cardholder password after a specified number of failed authentication attempts.																

- When you have completed your modifications, click **Submit**.

The message “Issuer Configuration Parameters updated” appears.

Managing Administrators and Issuer Administrators

Issuer administrators can perform tasks which manage and control other administrators and Issuer administrators. They can also view the administrator system access reports. This section discusses the following topics:

- Managing Issuer Administrator Accounts
- Managing CSR Accounts
- Viewing Administrator System Access Reports.

Managing Issuer Administrator Accounts

Issuer Administrators create and manage other Issuer Administrators. Issuer Administrators can perform the following tasks associated with managing Issuer Administrator accounts:

- Create Issuer Administrator accounts. See [“Creating Administrators and Issuer Administrators” on page 26](#) for detailed instructions.
- Update administrator privileges for a selected Issuer Administrator. See [“Updating Administrator \(CSR\) and Issuer Administrator Privileges” on page 30](#) for detailed instructions.
- Configure Issuer Administrator password policy. See [“Configuring Administrator Password Policy” on page 34](#) for detailed instructions.
- Enable or disable Issuer Administrator accounts. See [“Enabling/Disabling Administrators” on page 32](#) for detailed instructions.
- Reset Issuer Administrator passwords. See [“Resetting Administrator Passwords” on page 33](#) for detailed instructions.

Managing Administrator (CSR) Accounts

Issuer Administrators can be responsible for creating and managing Administrator accounts. See [“Advanced Authorization” on page 14](#) for more information. You can define a default set of privileges for all Administrators, and adjust the privileges for individual Administrator accounts.

Issuer Administrators can perform the following tasks associated with managing Administrator accounts:

- Create Administrator Accounts. See [“Creating Administrators and Issuer Administrators” on page 26](#) for detailed instructions.
- Update Administrator Privileges for a Selected Administrator. See [“Updating Administrator \(CSR\) and Issuer Administrator Privileges” on page 30](#) for detailed instructions.
- Enable or disable Administrator Accounts. See [“Enabling/Disabling Administrators” on page 32](#) for detailed instructions.
- Reset Administrator passwords. See [“Resetting Administrator Passwords” on page 33](#) for detailed instructions.
- Configure Administrator Password Policy. See [“Configuring Administrator Password Policy” on page 34](#) for detailed instructions.

Viewing Administrator System Access Reports

There are four reports you can use to retrieve and display information about Administrator and Issuer Administrator system use. You can choose to view a report online or export a report to a file to use in another software program.

NOTE:

This section provides instructions on how to view reports online. See [“Exporting a Report to a File” on page 22](#) for instructions on how to export a report.

The system displays reports according to the information set up in your Report Profile. See the [“Updating Your Profile” on page 21](#) for information on how to change your Report Profile.

This section divides the reports into the following categories:

- Administrator (CSR) System Access Reports. See [“CSR System Access Reports” on page 39](#) for detailed instructions.
- Issuer Administrator System Access Reports. See [“Issuer Administrator Account Reports” on page 41](#) for detailed instructions.

Chapter 5

Setting Up Issuer Accounts

This chapter discusses the different procedures you need to perform in order to set up an Issuer account. Only a Global Administrator with appropriate privileges can create and manage Issuer Accounts.

The procedure is divided into the steps mentioned below:

1. Perform pre-setup tasks.
2. Create an Issuer account.
3. Create Range Groups.
4. Add Financial Institution information for each supported card range to the Issuer account.

The following sections provide detailed instructions for each of the above tasks.

Pre-Setup Tasks

When you set up an Issuer account using the Administrative Console, you are asked for specific information regarding how the system should process authentications of different card ranges. To gather this information, perform the following pre-setup tasks:

- Generate the Issuer Data Encryption Key
- Define the Data Upload Tool passphrase.
- Obtain the CVV/CVC2 Key Pair Values.
- Obtain the HMAC key values for AAV calculations.
- Obtain the Issuer's Signing Certificate and Key information.
- Obtain the applicable Receipt Server or AHS information.
- Determining the crypto device supported.
- Determine the locales supported by the Issuer.
- Create an Issuer account directory.

The following sections provide detailed instructions for each of the pre-setup tasks.

Generating the Issuer Data Encryption Key

Issuer Data Encryption Keys are used to encrypt and decrypt data for the different Issuers you are hosting. Each unique Issuer you are hosting should have its own unique encryption keys (for example, MetroBank and United Bank should have their own unique encryption keys). Issuer accounts in different locales (for example, MetroBank-France and MetroBank-US), can share the same encryption keys.

If you are setting up more than one Issuer account, you can generate several encryption keys to draw from when setting up each Issuer. This will allow you to create a new Issuer account without restarting your system, which step is necessary whenever you create a new encryption key.

CAUTION:

If you choose to create several encryption keys, be sure to maintain a record of the labels corresponding to the keys you created and note to which Issuer each will be assigned. Arcot recommends that the encryption key for different Issuers be different.

You may use the Issuer Software `pk11_util` utility to generate encryption keys. See “[PK11 Util](#)” in [Chapter 6](#) for information on how to use this utility.

Determining the Data Upload Client Passphrase

If the Issuer will be using the Data Encryption Tool of the Data Upload Tool to encrypt cardholder data when it is uploaded to the Issuer Software Database, you need to define a passphrase for the tool. The passphrase is used to encrypt the cardholder data. The passphrase is a maximum of 23 printable ASCII characters. See the *Arcot Data Upload Tool for TransFort Installation and User Manual* for more information on setting the passphrase.

Obtaining the HMAC key for AAV Calculations*

The Accountholder Authentication Value (AAV) appears on a PARES confirming that cardholder authentication has been successfully performed. The key for AAV calculation is a Keyed-Hash Message Authentication Code. You can set the HMAC algorithm for AAV calculation at a card range level. See “[Adding Financial Institution Information to the Issuer Account](#),” for more information.

The actual key is created and stored in the cryptographic device. See “[Creating HMAC Keys for AAV](#),” for more information. The alias of the HMAC key, mapping to the appropriate key in the cryptographic device should be provided during Issuer setup.

You can also calculate the AAV using the CVC2 algorithm. See “[Obtaining the CVV/CVC2 Key Pair Values](#),” for more information.

Obtaining the BIN Key Identifier*

The Issuer must also obtain the BIN Key Identifier from MasterCard. The BIN Key Identifier indicates which one of the possible 16 issuer-known secret keys for a given BIN range was used by the ACS (identified by the `ACSIdentifierID` in `acs.ini`) to create the MAC.

See “[AAV Calculation and Instance Settings](#),” in the “[ACS Configuration File \(acs.ini\)](#),” for more information about the ACS Identifier. If you do not set the AAV algorithm during issuer setup, the ACS takes the configuration from the `acs.ini`. The values for this field are:

**.Applicable only for MasterCard configurations.*

- 0 – 7 Reserved for HMAC
- 8 – 15 Reserved for CVC2
- 16 – 255 – Reserved for future use

If the value is not present in the `acs.ini`, the default is 0 which indicates HMAC.

It is recommended that any given key associated with each identifier be maintained during the time that a charge back can occur. New keys can be rolled into the system by selecting a new identifier value.

Obtaining the CVV/CVC2 Key Pair Values

The Cardholder Verification Value (CVV) Keys are single-length DES key pairs used to calculate CAVVs. The CAVV, a Visa defined value, appears on a PAREs to confirm cardholder authentication was performed. The HSM uses the Cardholder Verification Value (CVV) algorithm to calculate the key values. Obtain the CVV key pair values following the procedure established by the Issuer. See “[Key Util](#),” to generate CVV keys.

If you are using the CVC2 algorithm to calculate the AAV, you should obtain the CVC2 key pairs. The Card Verification Code 2 (CVC2) keys are a pair of 64-bit DES secret keys identified by the **BIN Key Identifier** sub field. If you are using the HMAC keys to calculate the AAV, see “[Obtaining the HMAC key for AAV Calculations](#).”

Obtaining the CVV Key Indicator*

The CVV keys are periodically changed to enhance security. During the transition period, both the CVV key pairs are supported by Visa. Arcot Transfort Issuer Software supports only one key pair at a time. The CVV Key Indicator indicates the key pair used to calculate the CAVV values during purchase transactions.

For example, if an Issuer is using a particular CVV Key pair and has set the CVV Key Indicator to 01. When the Issuer wants to rotate the CVV Keys, the keys have to be updated and the CVV Key Indicator Value has to be toggled to 02.

Obtaining the Signing Certificate

You need the path and file name of an X509 certificate to use for signing the Payer Authentication Response (PAREs) during transaction authentication.

For information on how to create a signing key on the applicable cryptographic device and generate a signing certificate request file, see “[PK11 Util](#)”.

**.Applicable only for Visa configurations.*

For information on how to load an existing signing key into the applicable cryptographic device, see [“Key Util”](#).

Obtaining the Receipt Server Information

You need to obtain the URL of the Receipt Manager or AHS to use for receipts. The AHS URL is the only piece of AHS data you need to set up an Issuer account. Other AHS information is entered globally for the ACS. See [“Obtaining the AHS Certificates and Key” on page 144](#) for more information.

NOTE:

If you don't want to send the receipts to any receipt server, you can enter `http://none` or `https://none` in the receipt server field. The ACS detects this url and will not attempt to send the receipt.

Determining the crypto device supported

You can choose the crypto device supported to store the sensitive encryption keys, signing keys and keys for the chip key (when you use the chip card). You can also choose the cryptographic device for the storing the CVV/CVC2 and HMAC keys for CAVV and AAV calculations. You can setup the system to support more than one cryptographic device. See the [“Updating the Access Control Server Configuration,”](#) for more information. You need to provide the device for issuer keys and CVV/CVC2 keys at the issuer level (see [“Creating an Issuer Account,”](#)) and the signing keys, the CVV/CVC2 keys (for range level support) and the chip keys at the range level (see [“Adding Financial Institution Information to the Issuer Account,”](#)).

You can choose from the following cryptographic devices:

- nFast from nCipher
- Zaxus
- IBM 4578*
- IBM CCA*

NOTE: You must to configure the device you are selecting from the [HSM<N>DeviceName](#) field in the Update ACS Config page, before you configure the device here.

**.Supported only on AIX systems*

Determining the locales supported by the Issuer

You can set up an Issuer to support more than one locale. Obtain a list of supported locales and determine the default locale before creating the Issuer account. See *Arcot TransFort Issuer Software Introduction Manual* for more information.

Creating the Issuer Account Directory

The Issuer account directory contains the HTML, GIF, and certain JSP files for the Issuer's Enrollment site. Each Issuer supported by the Enrollment Server must have its own account directory.

The Issuer Software installation process creates a folder called `memberbank` in the:

- For Windows:

```
<$System Root$>:\CATALINA_HOME\vpas\webapps
```

- For Unix:

```
/opt/arcot/
```

directory that you can use as a template for the Issuer account directory.

See “[Customizing the Issuer's Enrollment Site](#)” in [Chapter 6](#) for information on how to customize the Enrollment site files.

To create an Issuer account directory:

1. Locate the following directory:

```
<%System Root%>:\CATALINA_HOME\webapps\vpas\memberbank
```

or

```
/opt/arcot/memberbank
```

2. Copy the **memberbank** directory and paste it into the following directory:

```
<%System Root%>:\CATALINA_HOME\webapps\vpas
```

or

```
/opt/arcot/
```

3. Rename this sub-directory to the desired directory name for the new Issuer account (for example, `metrobank`).

NOTE:

The directory name should not contain any white spaces or upper case characters.

Creating an Issuer Account

This function allows you to create the name that identifies the Issuer in the Issuer Software and assign miscellaneous Issuer-specific information to the account.

To create an Issuer account:

1. In the Administrative Console, click the **Create Issuer** link.

The *Create Issuer* page appears.

2. Enter the appropriate data in the applicable fields.

The following table provides descriptions of the fields on this page:

Table 5-1 Create Issuer fields

Field	Description
Issuer Name	The Issuer account name (for example, MetroBank). The Issuer Name value should be unique for each Issuer account you set up. For example, if the same Issuer is located in different locales, use the Issuer Name to indicate this, as in MetroBank-France, MetroBank-US, and so on.
Country	The country in which the Issuer operates.
Default Locale	The default locale associated with this Issuer account. See “Determining the locales supported by the Issuer” on page 72 for more information.
Local Time Zone	The time zone to use for Issuer reports. The Issuer Software Database stores applicable data with GMT time zone information. Specifying a Local Time Zone offsets the GMT data with the local time data in reports.
ES Issuer Directory	The Issuer account directory name (for example, metrobank). See “Creating the Issuer Account Directory” on page 72 for detailed information.
Encryption Key	The encryption key or label name created assigned to this Issuer. See “Generating the Issuer Data Encryption Key” on page 68 for detailed information.
Pass phrase	The encryption key used to encrypt data during upload. See “Determining the Data Upload Client Passphrase” on page 69 for more information.

Table 5-1 Create Issuer fields

Field	Description
User Encoding	<p>Specifies the language encoding used by exported administrator reports. Options available are as follows:</p> <ul style="list-style-type: none"> • ISO-8859-1Western Characters (default) • Big5Traditional Chinese • SJISJapanese • EUC_KRKorean
CVV/CVC2 Key A	<p>The encrypted value of the CVK A of the CVK pair. This value is generated on the HSM and is the first value of the pair generated.</p> <p>See “Obtaining the CVV/CVC2 Key Pair Values” on page 70 for more information.</p>
CVV/CVC2 Key B	<p>The encrypted value of the CVK B key of the CVK pair. This value is generated on the HSM and is the second value of the pair generated.</p> <p>See “Obtaining the CVV/CVC2 Key Pair Values” on page 70 for more information.</p>
Bank Key Module	<p>The crypto device used to store the bank encryption key. The options available are:</p> <ul style="list-style-type: none"> • nCipher - nShield • IBM Crypto Card - ibm4758 <p>NOTE: You must to configure the device you are selecting from the HSM<N>DeviceName field in the Update ACS Config page, before you configure the device here.</p>
Authentication Key Module	<p>The crypto device used to store the CVV/CVC2 keys. The options available are:</p> <ul style="list-style-type: none"> • nCipher - payshield • IBM Crypto Card - cca <p>NOTE:You must to configure the device you are selecting from the HSM<N>DeviceName field in the Update ACS Config page, before you configure the device here.</p>
Processor Name	The name of the transactions processor for the Issuer.

Table 5-1 Create Issuer fields

Field	Description
Sub Processor Name	The name of the sub-processor for the Issuer.
Processor Data	Specific data about the processor for the Issuer.
Processor Info	Any Additional information about the processor.
CVV Key Indicator	<p>An indicator to specify the CVV key pair used during periodic transition of CVV keys. See “Obtaining the CVV Key Indicator” on page 70 for more information.</p> <p>The options are:</p> <ul style="list-style-type: none"> • Not Configured - choose this if the CVV keys are configured at the range level or instance level. • 01 • 02
Locales Supported	<p>The list of locales supported by the Issuer. See “Determining the locales supported by the Issuer” on page 72 for more information. Select the locales supported from the drop down box. To select multiple locales, press and hold Ctrl while selecting the desired locales and then click >>>>.</p>
Do Not Prompt Behavior	<p>An indicator to specify how to handle Do Not Prompt during ADS.</p> <p>The options are:</p> <ul style="list-style-type: none"> • N in VERes • Attempts PAREs
User Id Supported	Indicates if the User Id is supported.
Two-Step Login Enabled	Indicates if Two-Step Login is enabled..
List of Global Admins	<p>The list of all the global administrators is shown on the left. Select the particular administrator you want to assign to the Issuer.</p> <p>To add a Global Administrator to support the Issuer, scroll through the List of Admins and select an administrator ID, then click >>>>. The administrator ID appears in the Selected Global Admins box. To select multiple admins, press and hold Ctrl while selecting the desired administrators and then click >>>>.</p> <p>NOTE: The Global administrator creating the Issuer automatically gets assigned to the new Issuer.</p>

Table 5-1 Create Issuer fields

Field	Description
List of Selected Admins	The list of Global Administrators selected to support the Issuer. To remove a Global Administrator from an Issuer account, select an administrator ID and click <<<<. The administrator ID is removed from this list. To remove multiple administrators, press and hold Ctrl while selecting the desired administrators and then click <<<<.

3. When you have completed entering information in the fields, click **Submit**.

The message “Issuer <Issuer name> added” appears.

Figure 5-1 Create Issuer Screen

Create Issuer

Fill up the following parameters appropriately and click **Submit** to create an Issuer.
Then add FI Information for each Card Range.

Issuer Name	<input type="text"/>
Country	-- --
Default Locale	-- --
Local Time Zone	PST (GMT-08:00)
ES Issuer Directory	<input type="text"/>
Encryption Key	<input type="text"/>
DU Passphrase	<input type="text"/>
Re-type DU Passphrase	<input type="text"/>
User Encoding	ISO-8859-1
CW/CVC2 Key A	<input type="text"/>
CW/CVC2 Key B	<input type="text"/>
Bank Key Module	NCipher - NShield
Authentication Key Module	NCipher - PayShield
Processor Name	<input type="text"/>
Sub Processor Name	<input type="text"/>
Processor Data	<input type="text"/>
Processor Info	<input type="text"/>
CVV Key Indicator	Not Configured
Do Not Prompt Behavior	N in VERes
Locales Supported	-- -- Thai-Thailand French-Canada Spanish-North America
User Id Supported	<input type="checkbox"/>
Two-Step Login Enabled	<input type="checkbox"/>

[List Of Global Admins](#)

[List Of Selected Global Admins](#)

Updating Issuer Information

Once you have created an Issuer account, you may update all fields except Country, Default Locale, ESIssuerDirectory and Encryption Key fields.

To update an Issuer:

1. Click the **Update Issuer** link.

The *Update Issuer* page appears.

2. Use the **Issuer** drop-down list to select the desired **Issuer account**.

The system populates the page with data that has previously been added for this Issuer account.

3. Update the applicable fields as needed.

See [Table 5-1 “Create Issuer fields”](#) for information on these fields.

4. When you have completed updating the fields, click **Submit**.

The message “Issuer Updated” appears.

Creating Range Groups

Range Groups is a feature that reduces administrative overhead by allowing a group of ranges to be configured as a single entity.

You can create and configure Range Groups. These range groups can be used across Issuers. The Issuer's independent card ranges can be associated with any one of the range groups created. The range groups can be configured for the following:

- **Enrollment**

See “[Configuring the Enrollment Process](#),” for more information.

- **Callouts**

See “[Configuring CallOuts](#),” for more information.

- **ACS-CAP Templates.**

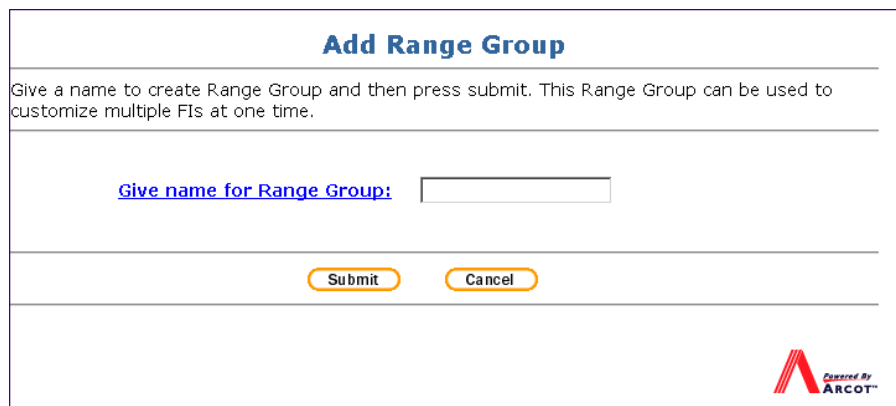
See “[Adding Issuer Template Customization](#),” for more information.

To create a range group:

1. Click on **Add Range Group** link

The *Add Range Group* page appears.


Figure 5-2 Add Range Group page



Add Range Group

Give a name to create Range Group and then press submit. This Range Group can be used to customize multiple FIs at one time.

[Give name for Range Group:](#)

 Powered By ARCOT™

2. Enter an appropriate name for the Range group you want to create and click **Submit**.

The message “Range Group created successfully” appears.

3. The Range Groups are associated with card ranges created using the Add FI Info page. They should be customized for enrollment, callouts and templates.

This makes the customization required for the Issuer very simple. The following section explains the range group feature with an example.

The Issuer Configuration Summary report displays the Range Group level configuration for a particular Issuer. See the *Arcot TransFort Issuer Software Reports Manual* for more details.

IMPORTANT:

The enrollment url for the range groups should include the range group id. See [“Configuring for a Specific Range or Range Group” on page 103](#) for more information on the enrollment URL.

Configuring Range Groups

An Issuer can have multiple card ranges belonging to multiple card types. The Issuer can create many card ranges and customize each range or can use the Range Group feature and reduce customization required.

The names of the Range Groups are available across Issuers. The Range Group can be configured for a particular Issuer. If another Issuer chooses to use the same Range Group, the Issuer must configure the group for all the parameters described in the previous section.

The following procedure describes how to use the range group feature:

1. You can create two Range Groups using the [“Add Range Group page,”](#) called *Visa Ranges* and *MasterCard Ranges*.
2. All the card ranges for the Issuer have to be entered into the system using the Add FI Info page in the administrative console.

See [“Adding Financial Institution Information to the Issuer Account,”](#) for more information.

3. Every range should be associated with one of the Range Groups created using the [Add to FI Group](#) field in the Add FI Info page—the Visa Cards can belong to the *Visa Ranges* and the MasterCard cards to the *MasterCard Ranges*.

The Issuer can have the following types of configuration:

- Only Range Group Configurations
- Only Range Configurations

- Configuring for Ranges associated with Range Groups

The sections below explain the configuration options in detail.

4. When you select the Issuer for whom you want to configure enrollment, templates or callouts, the “[Select a Range Page](#)” appears.

The Range Groups can be selected for all configuration purposes from the “[Drop-down Menu for Range Groups](#)”. The Ranges are selected from the “[Drop-down Menu for Ranges](#).”

Figure 5-3 Select a Range Page

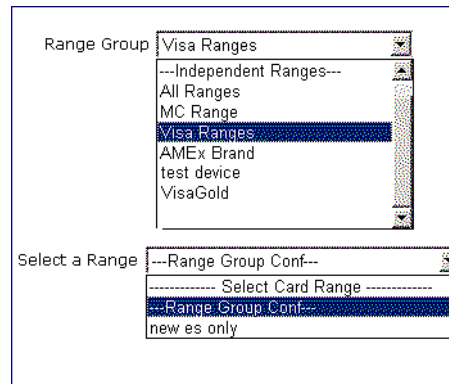
Figure 5-4 Drop-down Menu for Range Groups

Figure 5-5 Drop-down Menu for Ranges

Configuring for Range Groups only

The Range Groups can be configured for enrollment processes, templates and callouts. For the above example, if you want to configure for the *Visa Ranges* Range Group, select *Visa Ranges* from the Range Group drop-down and then select *--Range Group Conf--* from the select a Range drop-down menu. The **Range Group Conf** option in the menu lets you configure for the entire Range Group you have selected from the Range Group drop-down menu. See the figure below:

Figure 5-6 Configuring Range Group only



Configuring for Ranges only

If you want to configure for an independent range which is not associated with any Range Groups, choose the *--Independent Ranges--* option from the Range Group drop-down. The **Independent Ranges** option in the menu lets you select the ranges which are not associated with any Range Groups.

The **Select a Range** drop-down now displays only the ranges which are not associated with any Range Groups. Select the range for which you want to configure and proceed. In the figure below, the configuration is only for the *4015 range*.

Figure 5-7 Configuring Range Group only

Range Group: ---Independent Ranges---

Select a Range: ----- Select Card Range -----

Configuring for Ranges associated with Range Groups

An Issuer can associate multiple card ranges with a Range Group. The Range Group feature provides the flexibility to configure a range independently even after it is associated with a group. You have to first configure the Range Group as described in the earlier sections and then configure the particular ranges under the Range Groups to behave differently.

IMPORTANT:

The range configurations always takes priority over the Range Group Configuration.

You have to choose the Range Group to which the card range you want to configure belong from the **Range Group** drop-down menu. The **Select a Range** drop-down now displays the card ranges associated with the particular range group (Figure 5-8). Select the card range you want and proceed with the configuration.

Figure 5-8 Configuring a range within a Range Group

Range Group: MC Range

Select a Range: ----- Select Card Range -----

Adding Financial Institution Information to the Issuer Account

You need to add financial institution information for each card range supported by an Issuer. This information includes cardholder identification policy, chip card access, and external screening methods.

To add financial information to a card range:

1. Click the **Add FI Information** link.

The *Add FI Information* page appears.

This page is separated into three sections.

- a. Section 1 allows you to define card type, length, range, etc. for a specified card range.
- b. Section 2 allows you to define branding logos, signing certificates, authentication options, smart card access, and receipt server usage for the specified card range.
- c. Section 3 allows you to configure the Issuer Software for ADS and Enrollment Logging.

You cannot update the **Begin Range**, **End Range** and the **PAN length** once you submit the page. You may update all other fields on this page after submission via the *Update FI Information* link.

2. Enter the appropriate information in the applicable fields.

Figure 5-9 Add FI Info Page - Section 1

Issuer	<input type="text" value="----- Select Issuer Name -----"/>	
Card Range	<input type="text" value="----- Select Card Range -----"/>	Card Range Name <input type="text"/>
Add to Range Group	<input type="text" value="Default Group"/>	
Business ID	<input type="text"/>	FI Bin <input type="text"/>
Card Type	<input type="text" value="VISA Credit Card"/>	PAN Length <input type="text" value="16"/>
Begin Range		End Range
Term Policy Version	<input type="text" value="1"/> <input type="text" value="0"/>	Mobile Enabled <input type="text" value="Yes"/>
Signing Key Module	<input type="text" value="NCipher - NShield"/>	Authentication Key Module <input type="text" value="None"/>
Chip Key Module	<input type="text" value="None"/>	AAV Algorithm <input type="text" value="None"/>
SecureCode Key ID	<input type="text" value="0"/>	SecureCode Key Alias <input type="text"/>

The following table provides descriptions of the fields in Section 1:

Table 5-2 Add Financial Institution Information - Section 1 fields

Field	Description
Issuer	The name of the Issuer account for which you are adding data.
Card Range Name	Name given to the card range. This is an optional field and the name given is not enforced to be unique in the system. The value can be upto 65 characters.
<p>NOTE: If the card range name is set, this value appears in all the places in the administrative console instead of the card range.</p> <p>WARNING Hence it is strongly recommended that the name chosen for the card range is unique and informative. For example, the name string can be appended with the FI BIN - Gold Card (409971).</p>	
Add to FI Group	Choose a FI group to which you want to attach the current range. See “Creating Range Groups” on page 80 for more details.
Business ID	The 8-digit member identifier used to identify this Issuer.
FI BIN	The 6-digit BIN identifier assigned to the Issuer.

Table 5-2 Add Financial Institution Information - Section 1 fields

Field	Description						
Card Type	Specifies the type of cards that this card range covers. Options are: <ul style="list-style-type: none"> • Visa Credit Card • Visa Debit Card • MasterCard Credit Card • MasterCard Debit Card 						
PAN Length	The length of the Primary Account Number (PAN) that will be used with this card range. This length can be between 13 and 19 digits long.						
Begin Range	The first card number within the range of cards you are setting up.						
End Range	The last card number within the range of cards you are setting up.						
Term Policy Version	The version of the Issuer's Terms and Conditions policy to be used.						
Mobile Enabled	Specifies whether the specified card range will support mobile devices. Options are as follows: <table> <tr> <td>Yes</td><td>The card range will support mobile devices.</td></tr> <tr> <td>No</td><td>The card range will not support mobile devices.</td></tr> <tr> <td>Ask</td><td>The cardholder has the option of whether they want to use a mobile device.</td></tr> </table>	Yes	The card range will support mobile devices.	No	The card range will not support mobile devices.	Ask	The cardholder has the option of whether they want to use a mobile device.
Yes	The card range will support mobile devices.						
No	The card range will not support mobile devices.						
Ask	The cardholder has the option of whether they want to use a mobile device.						
Singing Key Module	The crypto device used to store the signing key used for signing the PAREs. The options available are: <ul style="list-style-type: none"> • nCipher - nShield • IBM Crypto Card - cca <p>NOTE: You must to configure the device you are selecting from the HSM<N>DeviceName field in the Update ACS Config page, before you configure the device here.</p>						

Table 5-2 Add Financial Institution Information - Section 1 fields

Field	Description
Authentication Key Module	<p>The crypto device used to store the CVV keys. The options available are:</p> <ul style="list-style-type: none"> • nCipher - payshield • Thales HSM • IBM Crypto Card - ibm4758 <p>NOTE:You must to configure the device you are selecting from the HSM<N>DeviceName field in the Update ACS Config page, before you configure the device here.</p>
Chip Key Module	<p>The crypto device used to store the chip keys. This option is used when you use the chip card method for authentication. The options available are:</p> <ul style="list-style-type: none"> • nCipher - payshield • Thales HSM <p>NOTE:You must to configure the device you are selecting from the HSM<N>DeviceName field in the Update ACS Config page, before you configure the device here.</p>
AAV Algorithm	<p>Select the algorithm to calculate the AAV. The options available are:</p> <ul style="list-style-type: none"> • HMAC - if you select this option, you must also provide the key identifier and the key alias. See “Obtaining the HMAC key for AAV Calculations,” for more information. • CVC2 - if you select this option you must specify the CVC2 keys and the CVV key indicator. See “Obtaining the CVV/CVC2 Key Pair Values,” for more information.
SecureCode Key ID*	<p>MasterCard’s BIN Key ID for the card range used for calculating the AAV’s. Its a numeric value from 0 to 15.</p> <p>See “Obtaining the BIN Key Identifier*,” for more information.</p>
SecureCode Key Alias*	<p>The alias string corresponding to the MC Key ID. You must provide an ID and alias if you want to use the HMAC method AAV calculation. If you dont provide these values here, the Authentication Key Module field is defaulted to nCipher - for CVC2 method.</p> <p>See “Obtaining the HMAC key for AAV Calculations,” for more information.</p>

*. Applicable only for MasterCard configurations.

The following table provides descriptions of the fields in Section 2:

Table 5-3 Add Financial Institution Information - Section 2 fields

Field	Description
Branding URL 1	<p>The location of the branding image file that is placed in image area 1 of the authentication page during a purchase.</p> <p>For example: member__logo.gif</p> <p>The system assumes this file is located in the <\$SystemRoot\$>:\Inetpub\wwwroot\acspage\<locale>\images directory.</p> <p>See “Customizing the Issuer’s Client Authentication Pages” in Chapter 7 for information on customizing this image file.</p>
Branding URL 2	<p>The location of the branding image file that is placed in Image area 2 of the authentication page during a purchase.</p> <p>For example: BankLogo.gif</p> <p>The system assumes this file is located in the <\$SystemRoot\$>:\Inetpub\wwwroot\acspage\<locale>\images directory.</p> <p>See “Customizing the Issuer’s Client Authentication Pages” in Chapter 7 for information on customizing this image file.</p>
ACS URL 1	<p>The URL for the primary ACS to be used for authentication. This URL must point to the <machine name>/acspage/cap. For example:</p> <p>ACS_Server1/acspage/cap</p>
ACS URL 2	<p>The URL for the secondary ACS (optional). This URL must point to the <machine name>/acspage/cap. For example:</p> <p>ACS_Server2/acspage/cap</p>
ACS URL 3	<p>The URL for the tertiary ACS (optional). This URL must point to the <machine name>/acspage/cap. For example:</p> <p>ACS_Server3/acspage/cap</p>
ACS URL 4	<p>The URL for the fourth ACS (optional). This URL must point to the <machine name>/acspage/cap. For example:</p> <p>ACS_Server4/acspage/cap</p>
ACS URL 5	<p>The URL for the fifth ACS (optional). This URL must point to the <machine name>/acspage/cap. For example:</p> <p>ACS_Server5/acspage/cap</p>

Table 5-3 Add Financial Institution Information - Section 2 fields

Field	Description
Signing Certificate File	The path and file name of the certificate used for signing the PAREs during a purchase transaction using 3-D Secure protocol. See “Obtaining the Signing Certificate” on page 70 for more information on this file.
Authentication Options	Specifies how the Issuer wants to allow cardholder authentication. Options are: <div> <div>Select</div> <div>Provides option buttons on the verification page during purchase transactions to the cardholder to select the method of authentication.</div> <div>Fallback</div> <div>Allows the cardholder to authenticate using the second authentication method if the cardholder failed using the first authentication method.</div> </div>
Authentication Priority	If the Fallback Authentication Option is selected, specifies the priority of the cardholder authentication methods. Options are: <div> <div>None</div> <div>If only one authentication method is required or if Authentication Priority is not important.</div> <div>Chip Card, Core</div> <div>If the authentication priority is chip card first followed by core password.</div> </div>
Max Auth Tries	The maximum number of tries for core password authentication before the transaction is declared failed. The value is also used for the Hint/Response or the Secret question feature used to support the <i>Forgot Your Password</i> feature.
Max Auth Tries Across Sessions	Indicates whether or not the Max Auth Tries is across sessions. This means that the authentication tries is counted across multiple transactions and not for a single transaction. The counter remains the same and is increased whenever a cardholder fails authentication in any transaction.
Max Auth Tries for Auto FYP	The number after which the FYP feature is automatically enabled. The “Auto FYP,” is a feature where the FYP is automatically enabled once the cardholder fails authentication for a configured number of attempts. This feature is enabled only in the case of a regular transaction. <div> <div>IMPORTANT:</div> <div>You should make sure this number is smaller than the “Max Auth Tries,” configured in the same page.</div> </div>
Chip Card	Indicates whether chip card authentication is available. Leave this box unchecked if you want core password only.

Table 5-3 Add Financial Institution Information - Section 2 fields

Field	Description
Plugin URL	If chip card authentication is selected, specifies the URL to the chip card plug-in installer.
Plugin Name	If chip card authentication is selected, specifies the name of the chip card plug-in.
Plugin Version	If chip card authentication is selected, specifies the version of the chip card plug-in to be used.
Smart Access Required	If chip card authentication is selected, indicates that smart access applications present on the chip card will be used for cardholder authentication.
HSM Variant	If chip card authentication is selected, indicates the HSM variant used. This is the Master Derivation Key (MDK) that is encrypted by the HSM's Local Master Key (LMK). Remove any white spaces in the generated HSM variant so that it is a continuous character string. See your HSM documentation for more information on this value.
Receipt URL	The URL to the Receipt Server or AHS that complies with the 3-D Secure protocol version 1.0.1 and version 1.0.2 DTD (or 1.0 messaging).
	<p>NOTE:</p> <p>If you don't want to send the receipts to any receipt server, you can enter <code>http://none</code> or <code>https://none</code> in this field. The ACS detects this url and does not attempt to send the receipt.</p>
CVV/CVC2 Key A	The encrypted value of the CVK A of the CVK pair. This value is generated on the HSM and is the first value of the pair generated. See “Obtaining the CVV/CVC2 Key Pair Values” on page 70 for more information.
CVV/CVC2 Key B	The encrypted value of the CVK B key of the CVK pair. This value is generated on the HSM and is the second value of the pair generated. See “Obtaining the CVV/CVC2 Key Pair Values” on page 70 for more information.

Table 5-3 Add Financial Institution Information - Section 2 fields

Field	Description
CVV Key Indicator	<p>An indicator to specify the CVV key pair used during periodic transition of CVV keys. See “Obtaining the CVV Key Indicator” on page 70 for more information.</p> <p>The options are:</p> <ul style="list-style-type: none"> • Not Configured - choose this if the CVV keys are configured at the issuer level or instance level. • 01 • 02

Figure 5-10 Add FI Info Page - Section 2

The following table provides descriptions of the fields in Section 3:

Table 5-4 Add Financial Institution Information - Section 3 fields

Field	Description
Auto Enroll Option	<p>The available methods for ADS. Select an option from the drop down list. See the <i>Arcot TransPort Issuer Software Introduction Manual</i> for more information.</p>

Table 5-4 Add Financial Institution Information - Section 3 fields

Field	Description
Max Declines	The number of times the cardholder can decline the Opt-in page to the online payer authentication program. See the <i>Arcot TransFort Issuer Software Introduction Manual</i> for more information.
Max Welcome	The number of times the cardholder views the Welcome page to the online payer authentication program. See the <i>Arcot TransFort Issuer Software Introduction Manual</i> for more information.
Enable VE Logging	If the check box is selected, the verify enrollment requests and responses (VEReq and VERes) are logged for the entire card range. See the <i>Arcot TransFort Issuer Software Introduction Manual</i> for more information. You can view the logs in the VELog report. For more details, see the <i>Arcot TransFort Issuer Software Reports Manual</i> .

- When you have completed entering information, click **Submit**.

The message “FI Information added” appears.

Figure 5-11 Add FI Info Page - Section 3

Updating the Financial Institution Information

Once you have added financial information to an Issuer account for a specified card range, you may update all fields except the **Begin Range**, **End Range**, and **PAN Length** fields. See the following tables for more information on updateable fields: [Table 5-2](#), [Table 5-3](#), and [Table 5-4](#).

To update financial institution for a card range:

- Click the **Update FI Information** link.

The *Update FI Information* page appears.

- Use the **Issuer** drop-down list to select the desired **Issuer account**.

The system makes existing card ranges available.

3. Use the **Card Range** drop-down list to select the desired **card range**.

The system populates the page with data that has previously been added for this card range.

4. Update the applicable fields as needed.

To disable a card range, select the **Disable Card Range** check box. This removes the selected card range from the 3-D Secure program. To enable the card range clear this check box.

5. When you have completed updating the fields, click **Submit**.

The message “FI Information updated” appears.

Chapter 6

Configuring the Enrollment Server

This chapter discusses the following topics:

- Updating the Enrollment Server Configuration
- Enrollment Process Pre Setup Tasks
- Configuring the Enrollment Process
- Configuring CallOuts
- Customizing the Issuer's Enrollment Site
- Configuring Forgot Your Password in ES

NOTE:

This chapter describes all possible tasks related to the enrollment server. Whether or not you have authority to complete the tasks described is defined by another Global Administrator or your Master Administrator.

Updating the Enrollment Server Configuration

The Enrollment Server Settings include:

- MIPS and IPGS Settings
- ES Cache Refresh Settings
- Callout Status Delimiter Settings
- Setting Administrator Session Timeout

MIPS and IPGS Settings*

The enrollment server configuration page has parameters to configure the MIPS parameters. The MIPS parameters and their description is given in the table below:

Table 6-1 MIPS Parameters configured for the Enrollment Server

Parameter	Description
mips.acqInstID	Acquirer Institution ID to be used in the \$1 Authorization.
mips.retries	Number of retries to the MIPS for a given request before abandoning.
mips.port	Port number for MIPS connection
mips.timeout	Time out in milliseconds for MIPS connection
mips.hostname	IP address of the host for MIPS connection

The IPGS parameter is defined in the `es.ini` file for the Enrollment Server in order for the IPGS communication to function. See “[ES Configuration File \(es.ini\)](#)” section in [Chapter 9](#) of this manual and the *Arcot TransPort Issuer Software Installation Manual* for information on updating this file.

This page enables global enabling or disabling IPGS communication for the Enrollment Server. The *GlobalIPGS* parameter is set to 1 to enable IPGS or 0 to disable IPGS. The IPGS defaults can also be set in this page. This action affects all Issuer accounts in the Issuer Software Database.

To update the Enrollment Server configuration:

1. Click the **Update ES Config** link.

The *Update ES Configuration* page appears.

**.MIPS parameters are applicable only to MasterCard and IPGS parameters are only applicable to Visa.*

2. Do any one of the following:
 - a. Set the GlobalIPGSON parameter for Visa
 - b. Set the MIPS parameters for MasterCard
3. Click **Submit**.

The message “ES Configuration Updated Successfully” appears.

4. Reboot all Tomcat instances.

Figure 6-1 ES Configuration Page

Update ES Configuration		
To configure system parameters across all Issuers, give the appropriate values and click Submit .		
Parameter Name	Value	Description
mips.acqInstID	01234	Merchant id used in mips connection
ipgs.defaults	D 4 473110 403731987	D 4 acquirer BIN (6) merchant number (12) store number (4) terminal number (4) device code (1) industry code
admin.timeout	300	Session timeout in minutes for admin users
ESCacheRefreshFrequency	1	Frequency (in minutes) at which ES/Admin Cache has to be refreshed. 0 indicates that refreshing is turned off.
mips.retries	2	Retries for mips
mips.timeout	1000	Time out in ms for mips connection
FORMAT_IN_CLAUSE_STRING	1	If system should try to optimize for long issuer list for reports
CalloutStatusDelimiter	,	Delimiter used for CalloutStatus column in ESLOG table
mips.port		Port number for mips connection
GlobalIPGSON	1	Global Admin sets this parameter for switching on/off IPGS for the entire system
mips.hostname		Host name for mips connection

Admin/Enrollment Server Cache Refresh

When the Admin/Enrollment Server service starts, it creates a cache of Issuer data to improve system performance. The administrator can refresh this cache by clicking on the *Refresh ES Cache* link. Only the Issuer information caches are refreshed through this action. The refresh will be automatically propagated to other instances of ES.

Table 6-2 Cache Refresh Parameter for the Enrollment Server

Parameter	Description
ESCacheRefreshFrequency	The time frequency in minutes after which the ES cache is refreshed. A value “0” for this parameter indicates that cache refresh do not happen.

Actions requiring ES Cache Refresh

The actions following which an ES cache refresh is required are listed below.

- Any addition, deletion or change to Issuer configuration.
- Any addition, deletion or change to Range configuration.
- Any addition, deletion or change to CallOut configuration.

Callout Status Delimiter Settings

CallOuts can log information in the TransFort system. The Enrollment Server logs can have information regarding the status of the callouts configured in the system. The reports which display the callout status use a delimiter set in this page to separate the multiple values returned by the callouts.

Table 6-3 CallOut Status Delimiter for Reports

Parameter	Description
CalloutStatusDelimiter	In all the reports where the Callout Status is displayed, if there are multiple values for the same, the values are delimited with the parameter set in this field.

Setting Administrator Session Timeout

The default session timeout value is ten minutes. This means the Administrative console will time out after an inactivity period of ten minutes is reached. The session time count starts only after a successful administrator login.

NOTE: The administrative session can timeout before report generation if you are generating reports with very large data. It is recommended that you increase the session timeout to a large number to complete the report generation.

The Update ES Config page allows you to set the time out parameter for the administrative console.

Table 6-4 Timeout parameter for Administrative Console Session

Parameter	Description
Admin.Timeout	The inactivity period in minutes after which the administrator's session from the console is timed out.

Enrollment Process Pre Setup Tasks

When you begin with the enrollment configuration using the administrative console, you are asked for specific information like cardholder identity verification policy, templates for the enrollment site, etc.

Perform the following pre setup tasks to obtain this information:

- Determining AVS and CVV2 Policy for Visa Configurations
- Determining AVS and CVC2 Policy for MasterCard Configurations
- Configuring for a Specific Range or Range Group

Determining AVS and CVV2 Policy for Visa Configurations

The Issuer has the option of defining one or more of the following policies for cardholder identity verification:

- Address Verification Service (AVS) Policy
- Card Verification Value 2 (CVV2) Policy

NOTE:

The AVS and CVV2 identification verification services are part of the Internet Payment Gateway System (IPGS). IPGS must be enabled before you can use these services.

For information on globally enabling or disabling IPGS, see [“Updating the Enrollment Server Configuration” on page 96](#).

Address Verification Service (AVS) Policy

The Address Verification Service verifies that the address supplied by the cardholder matches the billing address of the cardholder.

The Issuer can specify one or more of the following levels of authentication as acceptable for cardholder verification:

Table 6-5 Address Verification Service Response Code

Response Code	Description
A	Address matches, but ZIP code does not

Table 6-5 Address Verification Service Response Code

Response Code	Description
W	9-digit ZIP code matches, but address does not match
X	Exact match, address and 9-digit ZIP code match
Y	Address and 5-digit ZIP code match
Z	5-digit ZIP code matches, but address does not match

Card Verification Value 2 (CVV2) Policy

The Cardholder Verification Value 2 (CVV2) option determines the authentication status of a cardholder based on whether or not the cardholder correctly enters a three-digit verification code located on the signature panel on the back of the debit or credit card. This number does not show up on imprints of the card and is not added to the magnetic strip.

The Issuer can specify one or more of the following levels of authentication as acceptable for cardholder verification:

Table 6-6 Card Verification Value 2 Return Codes

Return Code	Description
M	CVV2 Match
P	Not Processed.
S	Merchant has indicated that CVV2 is not present on card.
U	Issuer not certified and/or has not provided Visa encryption keys

Determining AVS and CVC2 Policy for MasterCard Configurations

The Issuer has the option of defining one or more of the following policies for cardholder identity verification:

- Address Verification Service (AVS) Policy
- Card Validation Code 2 (CVC2) Policy

NOTE:

The AVS and CVC2 identification verification services are part of the Internet Payment Gateway System (IPGS). IPGS must be enabled before you can use these services.

Address Verification Service (AVS) Policy

The Address Verification Service verifies that the address supplied by the cardholder matches the billing address of the cardholder.

The Issuer can specify one or more of the following levels of authentication as acceptable for cardholder verification:

Table 6-7 Address Verification Service Response Code

Response Code	Description
A	Address matches, but ZIP code does not.
R	Retry, system unable to process
S	AVS currently not supported
U	No data from Issuer/Authorization system
W	For US addresses, nine digit postal code and address matches. For addresses outside the U.S., postal code matches, address does not.
X	For US addresses, nine digit postal code matches, address does not. For addresses outside the U.S., postal code and address match.
Y	Five digit postal code and address matches.
Z	Five digit postal code matches, address does not.

Card Validation Code 2 (CVC2) Policy

The Cardholder Validation Code 2 option determines the authentication status of a cardholder based on whether or not the cardholder correctly enters a three-digit verification code located on the signature panel on the back of the debit or credit card. This number does not show up on imprints of the card and is not added to the magnetic strip.

The Issuer can specify one or more of the following levels of authentication as acceptable for cardholder verification:

Table 6-8 Card Validation Code 2 Return Codes

Return Code	Description
M	Valid CVC 2 (match)
N	Invalid CVC 2 (non- match)
P	Unable to process
U	Issuer unregistered to process CVC 2

Table 6-8 Card Validation Code 2 Return Codes

Return Code	Description
Y	Invalid CVC 1 (only if track data is present)

Configuring for a Specific Range or Range Group

The enrollment process allows you to configure all the elements either for a specific card range or across many ranges - called Range Groups for a particular Issuer. See “[Creating Range Groups](#)” on page 80 for more information. There is no nesting or hierarchy between the two types of configurations.

If you want to use both levels of configuration then you must configure all the elements for both types of configuration.

For example, Member Bank has Visa and MasterCard ranges. You must create and configured two range groups *Visa Ranges* and *MasterCard Ranges* for enrollment. You can also configure all the specific card ranges.

You must configure all the elements like cardholder fields, attributes, password, callouts, etc. If the range group configuration for any element is not complete, the configuration will not use any range level configuration even though the range level configuration is available.

WARNING:

If you have configured for any specific card ranges and then choose to configure for any specific range groups, you may see some default values on the screen. These values do not reflect any range level configuration. You must choose the configuration and click **Submit** to configure the range groups.

Choosing the Enrollment URL

The enrolment site will reflect the configuration depending on the URL chosen. If the enrollment URL uses the *range ID*, then the enrollment configuration is from the chosen range configuration. Alternately if the URL uses the *range group ID*, the range group enrollment configuration is displayed.

NOTE:

It is important to use the appropriate URL depending on the type of configuration. The Issuer ID and the range ID is passed in the URL. If you configure only the range groups individually for an Issuer and the enrollment site URL uses the range ID (and you have not configured for specific range), then there will be an error.

Landing Page for Enrollment URL

A *landing page* is provided to map the card number to the appropriate card range and corresponding template. See the *Arcot TransFort Issuer Software Introduction Manual* for more details. The landing page initially locates the range level configuration. If you have configured the card ranges individually the landing page uses the range level enrollment configuration. If there is no range level configuration available for the range, then the range group configuration is used. If both are not available, there will be an error.

Configuring the Enrollment Process

The enrollment process involves configuring parameters like:

- Cardholder fields for Enrollment
- Issuer Questions and the Question Policy
- Cardholder Password Policy
- Steps of Enrollment

A Global Administrator can configure the enrollment process for Issuer Accounts through the *Enrollment Process Configurations* links from the administrative console. The global administrator must have operative control over the Issuer to configure the enrollment parameters. See “[List of Global Admins](#),” in [Table 5-1 “Create Issuer fields”](#) for more details on how to assign an issuer to a global administrator.

The configuration of these parameters affect how the Issuer Enrollment Web site performs certain functions during enrollment. The enrollment parameters which are configured are classified into the following:

- Cardholder Fields and Abridged Fields
- Order and Abridged Order
- Attributes
- Password
- Issuer Questions
- Question Policy

Common Tasks for enrollment process.

The following steps are common across all the links mentioned above. To configure the enrollment process:

1. Click on the required link to configure any specific enrollment process.
2. Select the Issuer to be configured and press **Submit**.
3. Select the appropriate card range or the range group to be configured for the Issuer and press **Submit**. See “[Configuring for a Specific Range or Range Group](#),” for more details.

4. The specified page appears.

Configure the required parameters and press **Submit**.

WARNING:

Some default values may be shown on the screen. This does not mean that they are saved to database. So you must click **“Submit”** the first time you configure a range. This configuration is a must for your enrollment to start.

5. To continue configuring for the same Issuer-card range combination, choose the required links from the header of the page.

All the changes will affect only the card ranges of the Issuer you choose in steps 2 and 3.

CAUTION:

An Issuer must define the exact configuration of cardholder enrollment parameters *before* allowing cardholder enrollment to begin. Issuers are not expected to alter any of the cardholder enrollment parameters after cardholders have completed the enrollment process.

The following sections provide more details about the enrollment process.

Configuring Cardholder Fields for Standard and Abridged Enrollment

The fields to be shown during standard and abridged enrollment are configured using the **Fields** link. See **“Abridged Enrollment” on page 47 in Chapter Chapter 3** for more information. The fields are configured to be shown in one or two steps during standard enrollment. The first step of enrollment is called the *Identification Step* (also called the Card Number step) and the second step is called *Cardholder Verification Step* (also called Attributes step). See **Table 6-10 “Enrollment Steps”** for more details.

Some of the fields have certain default properties:

- **Card Number** is always selected, mandatory and will be asked in the Identification Step.
- **Name on Card** is always mandatory if selected.

To configure the fields:

1. Click on the **Fields** link under the **Configure Enrollment Process** heading.

The *Select Cardholder Enrollment Fields* page appears.

2. The page is divided into seven columns:

Table 6-9 Cardholder Enrollment Fields

Column	Description
Prompt	Select the check box in this column for the corresponding field to appear during <i>standard enrollment</i> .
Prompt (Abr)	Select the check box in this column for the corresponding field to appear during <i>abridged enrollment</i> .
Field Name	The name of the field.
Mandatory	Select this check box if you want the response of this field to be mandatory.
<p>NOTE: Some fields of this column are pre-determined to be mandatory.</p>	
Display Format	Some fields can have different formats of display. Choose the available format from the drop down box.
In Identification Step	Select the check box in this column for the corresponding field to appear in the Identification Step during <i>standard enrollment</i> . If left clear, the field will appear in the Cardholder Verification Step.
In Identification Step(Abr)	Select the check box in this column for the corresponding field to appear in the Identification Step during <i>abridged enrollment</i> . If left clear, the field will appear in the Cardholder Verification Step.

3. Select the configuration of fields you want and press **Submit**.

The message “Enrollment Fields updated Successfully” appears.

Figure 6-2 Cardholder Enrollment Fields Page

Is	Order	Attributes	Password	Issuer Questions	Question Policy
--------------------	-----------------------	----------------------------	--------------------------	----------------------------------	---------------------------------

Select Card Holder Enrollment Fields

the card holder attributes for the enrollment process, check mandatory to make the fields mandatory, select a format for special fields and select if you want them to be shown on Identify step.

Prompt	Prompt (Abr)	Field Name	Mandatory	Display Format	In Identification Step	In Identification Step (Abr)
Y	Y	Card Number	Y	none	Y	Y
<input type="checkbox"/>	<input type="checkbox"/>	Social Security Number	<input type="checkbox"/>	none	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Send Promotional Emails	<input type="checkbox"/>	none	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	Billing Address	<input type="checkbox"/>	none	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	DL Number	<input type="checkbox"/>	none	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	Expiration date	<input type="checkbox"/>	mm/yyyy	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	Home Phone Number	<input type="checkbox"/>	none	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	Is Phone Listed	<input type="checkbox"/>	none	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Name on Card	Y	NAME_3	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	Date of Birth	<input type="checkbox"/>	mm/dd/yyyy	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	DL State	<input type="checkbox"/>	none	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	State	<input type="checkbox"/>	none	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Email	<input type="checkbox"/>	none	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	Zip	<input type="checkbox"/>	none	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	Signature Panel Code	<input type="checkbox"/>	none	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	City	<input type="checkbox"/>	none	<input type="checkbox"/>	<input type="checkbox"/>

Configuring Order for Standard and Abridged Enrollment

Cardholder enrollment process can be combined into one or more steps. If the process is set to one page, the process of evaluation is from the top to the end of page the cardholder sees. The sequence of these steps can be configured through the **Order** link. A *step number* decides the sequence of steps. The cardholder will see the enrollment screens in increasing order of the step number. More than one step can have the same step number and will be shown to the cardholder together. Alternatively the step can be disabled and will not appear during enrollment.

NOTE:

The Identification Step and Attributes Step cannot be disabled.

Each step has its own function as described in the table below:

Table 6-10 Enrollment Steps

Enrollment Step	Description
Identification Step (Card Number)	This is the first step during the enrollment process. It is mandatory that the cardholder enters the card number at this stage. Any other fields can be configured to be shown in this step through the “Configuring Cardholder Fields for Standard and Abridged Enrollment,” link.
Terms and Conditions	The page will show the Issuer’s Terms and Conditions to the 3-D Secure program. The enrollment will proceed if the cardholder accepts the Terms and conditions.
Cardholder Verification Step (Attributes)	The cardholder is asked to enter personal information for identification in this step. The fields shown here are configured through the “Configuring Cardholder Fields for Standard and Abridged Enrollment,” link.
Cardholder Verification Step (Q&A)	The Issuer can configure a set of questions for the cardholder to answer in this step. Cardholder verification is done based on the responses to these questions. The Issuer questions is set through the “Setting Issuer Questions,” link.
Set Password	In this step, the cardholder is asked to set a secret password for verification during purchase transactions. Additionally the cardholder can also set a secret question and answer for authentication in this step. See “Configuring Cardholder Password Policy” on page 113 for more details about configuring the secret question and answer.
Set Personal Message	In this step the cardholder is asked to choose a personal message. This message appears during a purchase transaction and offers the cardholder assurance that the transaction is secure and valid.

To set the Cardholder Enrollment Sequence:

1. Click on the **Order** link under the **Configure Enrollment Process** heading.

The *Configure Enrollment Sequence* page appears.

2. To configure the order for standard enrollment, select the desired step numbers from the **Step Number** column.

To configure the order of abridged enrollment, select the desired step numbers from the **Step Number Abridged** column.

3. Press **Submit**.

The message “Steps updated successfully” appears.

Figure 6-3 Order of Enrollment Process Page

Fields	Order	Attributes	Password	Issuer Questions	Question
--------	-------	------------	----------	------------------	----------

Configure Enrollment Sequence

Select the steps you want in your enrollment process and sequence of these steps.

Step	Step Number	Step Number Abridged
Identification Step(Card Number)	1	1
Terms and Conditions	2	2
Card Holder Verification Step (Attributes)	3	3
Card Holder Verification Step(QA)	4	4
Set Password	5	5
Set Personal Message	6	6

URL For Enrollment is given below, change the locale, protocol or hostname as required.
https://10.150.1.129/vpas/enroll/index.jsp?locale=en_US&id=18&bankid=1

Configuring Enrollment Process Attributes

The attributes related to the enrollment process are configured through the **Attributes** link. The different attributes configured and their description is given in the table below:

Table 6-11 Enrollment Attributes

Attribute	Description
Enrollment Directory/Folder	<p>The ES Issuer directory is used in the login URL for Issuer administrators and CSRs (Administrators).</p> <p>The in-built options is:</p> <ul style="list-style-type: none"> bn - a Brand Neutral template <p>For example the login URL can be:</p> <p><code>https://<hostname>/vpas/admin/adminlogin.jsp?bank=bn</code></p> <p>WARNING: The directory name should not contain any white spaces.</p>

Table 6-11 Enrollment Attributes

Attribute	Description
Enrollment User Interface Template	Enrollment template will fetch you the page layout as well as i18n strings used as messages/error in enrollment. The in-built option is: <ul style="list-style-type: none"> • bn52- Brand Neutral template
Name of main logo	Issuer's main logo on the enrollment screen. The GIF files for the logo can be customized. See “Customizing the Issuer's Enrollment Site” on page 124 for more information.
Name of small logo	The Issuer's small logo on the enrollment screen. The GIF files for the logo can be customized. See “Customizing the Issuer's Enrollment Site” on page 124 for more information.
Re-Registration Allowed	Whether or not a previously registered cardholder may re-register a card in the 3-D Secure program. <p style="text-align: center;">CAUTION: Any previous cardholder information is overwritten during re-registration.</p>
\$1 Auth Required(MIPS/IPGS)	Whether or not the cardholder goes through the \$1 Authorization check during regular enrollment.
\$1 Auth Required for Abridged (MIPS/IPGS)	Whether or not the cardholder goes through the \$1 Authorization check during abridged enrollment.
\$1 Auth Step	The step name after which the \$1 Authorization is done. To ensure success of this authorization a minimum of three parameters have to be configured: <ul style="list-style-type: none"> • Card Number • Name on Card • Expiry Date <p>Make sure you configure the three parameters in the step prior calling the \$1 Auth.</p>

Table 6-11 Enrollment Attributes

Attribute	Description
Address Verification Service (AVS)	<p>The Address Verification System response codes that will be considered acceptable based on the Issuer's policy. To select more than one code, press and hold Ctrl as you select the desired code values.</p> <p>See “Address Verification Service (AVS) Policy” on page 100 for Visa AVS return codes.</p> <p>See “Address Verification Service (AVS) Policy” on page 102 for MasterCard AVS return codes.</p> <p>To ensure success of this service a minimum of four parameters have to be configured:</p> <ul style="list-style-type: none"> • Card Number • Name on Card • Billing Address • Zip Code <p>Make sure you configure the three parameters in the step prior using the service</p>
CVV2/CVC 2 check	<p>The Card Validation Code 2 return codes that will be considered acceptable based on the Issuer's policy. To select more than one code, press and hold Ctrl as you select the desired code values.</p> <p>See “Card Verification Value 2 (CVV2) Policy” on page 101 for Visa return codes.</p> <p>See “Card Validation Code 2 (CVC2) Policy” on page 102 for MasterCard return codes.</p> <p>To ensure success of this check a minimum of three parameters have to be configured:</p> <ul style="list-style-type: none"> • Card Number • Name on Card • Signature Panel Code <p>Make sure you configure the three parameters in the step prior using the check.</p>

To configure the attributes for enrollment:

1. Click on the **Attributes** link under the **Configure Enrollment Process** heading.

The *Configure Parameter/Policy for Enrollment* page appears.

2. Select the required configuration required and press **Submit**.

The message “Parameters updated successfully” appears.

Figure 6-4 Enrollment Attributes Page

Configure Parameters/Policy for Enrollment	
these are the parameters that will be used while enrollment, please provide them carefully.	
Name	Value
Enrollment Directory/Folder	bn
Enrollment UI Template	bn52
Mini-Enrollment Directory/Folder	
Mini-Enrollment UI Template	
Name of Main Logo	MCMemberBank.gif
Name of Small Logo	MCMemberBank-small.gif
Re-Registration Allowed	Yes
\$1 Auth Required(MIP/IPGS)	No
\$1 Auth Required for Abridged(MIP/IPGS)	No
\$1 Auth Step	None
Address Verification Service(AVS)	
CVV2/CVC2 check	

Configuring Cardholder Password Policy

The **Password** link enables the Issuer to set a password policy for the cardholder. The following table describes the password policy parameters.

Table 6-12 Cardholder Password Policy Parameters.

Parameter	Description
Secret Question/Answer Required?	Indicates whether or not the system should present the cardholder with a question and allow the cardholder to specify an answer after a configurable number of failed authentication attempts. If the cardholder enters the correct response, the system authenticates the user.
Minimum Length	The minimum number of characters that a password must have to be valid.

Table 6-12 Cardholder Password Policy Parameters.

Parameter	Description
Maximum Length	The maximum number of characters that a password may have to be valid.
Minimum Numeric	The minimum number of numeric characters that must be used in the password.
Minimum Alphabets	The minimum number of alphabetic characters that must be used in the password.
Minimum Special Characters	The minimum number of special characters that must be used in the cardholder's secret password. Special characters supported are: ! "# \$ % & ' () * +, -. /; < = > ? @ .

To configure the cardholder password policy:

1. Click on the **Password** link under the **Configure Enrollment Process** heading.
The “Specify Password Policy for Card Holders” page appears.
2. Select the desired configuration for the cardholder password and press **Submit**.
The message “Password Policy updated successfully.” appears.

Figure 6-5 Cardholder Password Policy

Fields	Order	Attributes	Password	Issuer Questions	Question Policy														
Specify Password Policy for Card Holders																			
Enable/Disable hint/response, password hint features by selecting from the list below, Specify password attributes that will be used while new enrollment and password change.																			
<table border="1"> <thead> <tr> <th>Card Holder Password Attribute</th><th>Value</th></tr> </thead> <tbody> <tr> <td>Secret Question/Answer Required</td><td>No <input type="button" value="v"/></td></tr> <tr> <td>Minimum Length</td><td>No Constraint <input type="button" value="v"/></td></tr> <tr> <td>Maximum Length</td><td>No Constraint <input type="button" value="v"/></td></tr> <tr> <td>Minimum Alphabet</td><td>No Constraint <input type="button" value="v"/></td></tr> <tr> <td>Minimum Numeric</td><td>No Constraint <input type="button" value="v"/></td></tr> <tr> <td>Minimum Special</td><td>No Constraint <input type="button" value="v"/></td></tr> </tbody> </table>			Card Holder Password Attribute	Value	Secret Question/Answer Required	No <input type="button" value="v"/>	Minimum Length	No Constraint <input type="button" value="v"/>	Maximum Length	No Constraint <input type="button" value="v"/>	Minimum Alphabet	No Constraint <input type="button" value="v"/>	Minimum Numeric	No Constraint <input type="button" value="v"/>	Minimum Special	No Constraint <input type="button" value="v"/>			
Card Holder Password Attribute	Value																		
Secret Question/Answer Required	No <input type="button" value="v"/>																		
Minimum Length	No Constraint <input type="button" value="v"/>																		
Maximum Length	No Constraint <input type="button" value="v"/>																		
Minimum Alphabet	No Constraint <input type="button" value="v"/>																		
Minimum Numeric	No Constraint <input type="button" value="v"/>																		
Minimum Special	No Constraint <input type="button" value="v"/>																		

Setting Issuer Questions

Upto ten questions can be specified for the cardholder to answer during the verification step. Standard questions include asking for the cardholder's mother's maiden name, city of birth, and so on. These questions are asked in the Cardholder Verification Step (QA).

Global Administrators define the number of questions a cardholder needs to answer correctly. For more information, see [“Configuring Question Policy” on page 116](#)

For more information on cardholder identity verification methods, see *Arcot TransFort Issuer Software Introduction Manual*.

To add or update Issuer questions:

1. Click the **Issuer Questions** link from the **Configure Enrollment Process** heading.

The *Add/Update Issuer Questions* page appears.

2. Choose the locale from the locale drop down list. You can configure questions for all the locales an Issuer supports.

WARNING: You must adhere of the question policy when you configure questions for multiple locales.

A single question policy applies to all the locales supported. See [“Configuring Question Policy,”](#) for more details.

IMPORTANT: The Failed Registrations Report displays the failed question ID's for a cardholder. Hence you should also ensure that the question ID's for similar questions in different locales are the same.

3. Type the desired **questions** in the provided text boxes and indicate whether or not the cardholder's response to each question should be case-insensitive or case-sensitive.
4. You can also mandate some or all questions from the check box. For these questions correct responses have to be provided the cardholder during enrollment.
5. Click **Submit**.

The message “Issuer Questions Updated Successfully” appears.

Figure 6-6 Add Issuer Questions Page

Fields	Order	Attributes	Password	Issuer Questions	Question Policy
Add/Update Issuer Questions					
Enter/Edit the questions the Cardholder should answer, select attributes of question/response and click Submit.					
Locale:		English-United States ▼			
Id	Mandatory	Issuer Question	Case Sensitivity of Response		
1	<input checked="" type="checkbox"/>	Mother's Maiden Name	Exact Match-Case Insensitive ▼		
2	<input checked="" type="checkbox"/>	Mailing Address 4 digit zip code	Exact Match-Case Sensitive ▼		
3	<input type="checkbox"/>		Exact Match-Case Sensitive ▼		
4	<input type="checkbox"/>		Exact Match-Case Sensitive ▼		
5	<input type="checkbox"/>		Exact Match-Case Sensitive ▼		
6	<input type="checkbox"/>		Exact Match-Case Sensitive ▼		
7	<input type="checkbox"/>		Exact Match-Case Sensitive ▼		
8	<input type="checkbox"/>		Exact Match-Case Sensitive ▼		
9	<input type="checkbox"/>		Exact Match-Case Sensitive ▼		
10	<input type="checkbox"/>		Exact Match-Case Sensitive ▼		

Configuring Question Policy

The Issuer can choose to ask cardholders up to ten questions to help prove that they are who they say they are. The responses are verified using data from the Issuer Software Database. This data must be pre-loaded into the Issuer Software Database using the Arcot Data Upload Client for TransFort. See the *Arcot Data Upload Client Installation and User Manual* for more information on this utility.

To configure the Issuer Question Policy:

1. Click on the **Question Policy** link under the **Configure Enrollment Process** heading.

The *Specify Card Holder Verification Policy* page appears.

2. Select the minimum number of question that a cardholder must answer correctly to proceed with enrollment. This minimum number will include the mandatory questions.

For example,

Total number of question = 3,

Number of Mandatory Questions = 2 and

Minimum Correct Answers = 3, then cardholder needs to answer all the three questions.

CAUTION: The minimum number of mandatory question set should not be greater than the total number of Issuer Questions.

When you configure questions for multiple locales, a single question policy applies to all the locales supported. You should consider this when you set the mandatory questions in the policy. For example:

Questions configured for Locale1 = 4

Questions for Locale2 = 2

Number of mandatory questions = 3

The question policy will not work for Locale2 as the number of questions configured is lower than the number of mandatory questions.

3. Select the type of evaluation for responses (only Internal Evaluation supported) and press **Submit**.

The message “Question Policy updated successfully” appears.

Figure 6-7 Cardholder Responses Verification Policy

Fields	Order	Attributes	Password	Issuer Questions	Question Policy						
<h3>Specify Card Holder Verification Policy</h3>											
Select various attributes for issuer questions including external evaluation from the lists below and then submit to save.											
<table border="1"><thead><tr><th>Policy</th><th>Value</th></tr></thead><tbody><tr><td>Minimum Correct Answers</td><td>2</td></tr><tr><td>Evaluation Approach</td><td>Internal</td></tr></tbody></table>		Policy	Value	Minimum Correct Answers	2	Evaluation Approach	Internal				
Policy	Value										
Minimum Correct Answers	2										
Evaluation Approach	Internal										

Configuring CallOuts

A Global Administrator can configure CallOuts invoked at run-time when certain pre-defined events occur. See *Arcot TransFort Issuer Software Introduction Manual* for more information. This section describes the following topic:

- [Adding CallOut Configuration](#)
- [Updating CallOut Configuration](#)
- [Adding CallOuts to an Issuer](#)
- [Updating an Issuer's CallOuts](#)

Adding CallOut Configuration

A Global Administrator needs to configure a CallOut in the system before using it at a card range level.

To configure a CallOut:

1. In the administrative console click on the **Add Callout Configuration** link.

The *Add CallOut Configuration* page appears.

Figure 6-8 CallOut Configuration Page

Add CallOut Configuration

This screen Adds/Updates CallOut Configuration

[CallOut Configuration Id](#)
[Destination URL](#)
[Connection Time Out](#)
[Response Time Out](#)
[Max Connection Tries](#)
[SSL Client Cert Path](#)
[SSL Root CA Cert Path](#)
[Encryption Cert](#)

CallOut Parameters

Parameter Name	Value
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

2. Enter the applicable data in the appropriate fields.

The following table provides descriptions of the fields on this page:

Table 6-13 CallOut Configuration Parameters

Field	Description
CallOut Id	The unique identification for the CallOut to be configured. This field is mandatory.
Destination URL	The URL to which the CallOut will be made. This URL is expected to implement the functionality for which it is registering.
Connection Time Out	Server socket connection time-out to CallOut URL in seconds. Default is 0.
Response Time Out	Server socket time-out on responses from CallOut URL in seconds. Default is 0
Max Connection Tries	The number of tries for connection to the CallOut URL. Default is 3.
SSL Client Cert Path	The path where the SSL client certificate is present
SSL Root CA Cert Path	The path where the Root CA certificate is present
Encryption Cert	The file is used to sign the CallOuts.
CallOut Parameters	The following text boxes are provided for data exchange between Issuer software and the callout. The parameters are stored as name-values pairs.
Parameter Name	Name of the callout parameter
Parameter Value	Corresponding value of the callout parameter.

NOTE:

By default there are five text boxes provided for the callout parameters. If you want more, click on **Add** below the text boxes. Five more boxes always appear.

WARNING

The name-value pairs are internally separated by a semi-colon (;). Do not use the semicolon (;) in the name- value pairs.

3. Click **Submit**.

The message “CallOut Added Successfully” appears.

Updating CallOut Configuration

The CallOuts already configured can be updated with this operation.

To Update a CallOut:

1. In the administrative console click on the **Update CallOut Configuration** link.
The *Update CallOut Configuration* page appears.
2. Choose the CallOut Id for which changes have to be made.
3. Make the necessary changes to the fields on the page. See [Table 6-13 “CallOut Configuration Parameters”](#) for details of the fields.
4. Click **Submit**.

The message “Updated CallOut Configuration” appears.

Adding CallOuts to an Issuer

Once you configure a CallOut, you need to assign it to the applicable Issuer.

To add a CallOut to an Issuer:

1. In the administrative console click on the **Add Issuer CallOut** link.
The *Add Issuer CallOut* page appears.

Figure 6-9 Add Issuer CallOut Page

Add Issuer Callout

Fill up the following parameters appropriately and click **Submit** to add an Issuer callout configuration.

Issuer Name	-- --
Range Group	--
Card Range	-- --
CallOut Type	-- --
CallOut Path	
Status	-- --
CallOut Configuration Id	-- --

Submit
Cancel

2. Enter the applicable data in the appropriate fields.

The following table provides descriptions of the fields on this page:

Table 6-14 Add Issuer CallOut Parameters

Field	Description
Issuer Name	Select the Issuer for which the CallOut has to be configured from the drop down list.
Card Range	Select the card range or range group of the Issuer for which the CallOut has to be configured.
<p>NOTE: You can select the All Ranges option to configure the callout across all ranges for the chosen Issuer.</p>	
CallOut Type	Select the type of CallOut from the drop down list. See the <i>Arcot TransFort Issuer Software Introduction Manual</i> for information about different types of CallOuts.
CallOut Path	The path of the class/dll which handles this CallOut and complies with CallOut interface.
Status	<p>This parameter decides if the CallOut has to be invoked or not.</p> <p>Enable: for the CallOut to be invoked.</p> <p>Disable: if the CallOut should not be invoked.</p> <p>Forced: You can use this status to invoke the VP Callout for chip card transaction irrespective of</p> <ul style="list-style-type: none"> • Transaction type(core, chip, ArcotID etc.) or • Cardholder status(with or without password in database) <p>When configured to Forced, the VP callout can be configured to prompt for the disconnected chip card random number and authenticate the cardholder.</p> <p>NOTE: This status is applicable only to the VP Callout. For any other callout this status is same as Enable.</p>
CallOut Configuration Id	The identifier of the CallOut being configured.

3. Click **Submit**.

The message “Issuer CallOut Added Successfully” appears.

Updating an Issuer's CallOuts

You can update CallOuts already added to a particular Issuer.

To update an Issuer CallOut:

1. In the administrative console click on the **Update Issuer Callout** link.

The *Update Issuer CallOut* page appears.

2. Choose the Issuer for which changes have to be made.
3. Make the necessary changes to the fields on the page.

See [Table 6-14 “Add Issuer CallOut Parameters”](#) for details of the fields.

4. Click **Submit**.

The message “Updated Issuer CallOut Successfully” appears.

Customizing the Issuer's Enrollment Site

Each Issuer can have its own customized Web pages for its Enrollment site and for the password pages that appear during a purchase transaction.

This section covers the following topics:

- Customizing the ES
- Customizing mini enrollment
- Customizing Enrollment site Graphics
- Customizing message files

Customizing the ES

The Enrollment Server has powerful customization abilities. The main components which are customized are:

- ES User Interface Template
- Enrollment Site Text

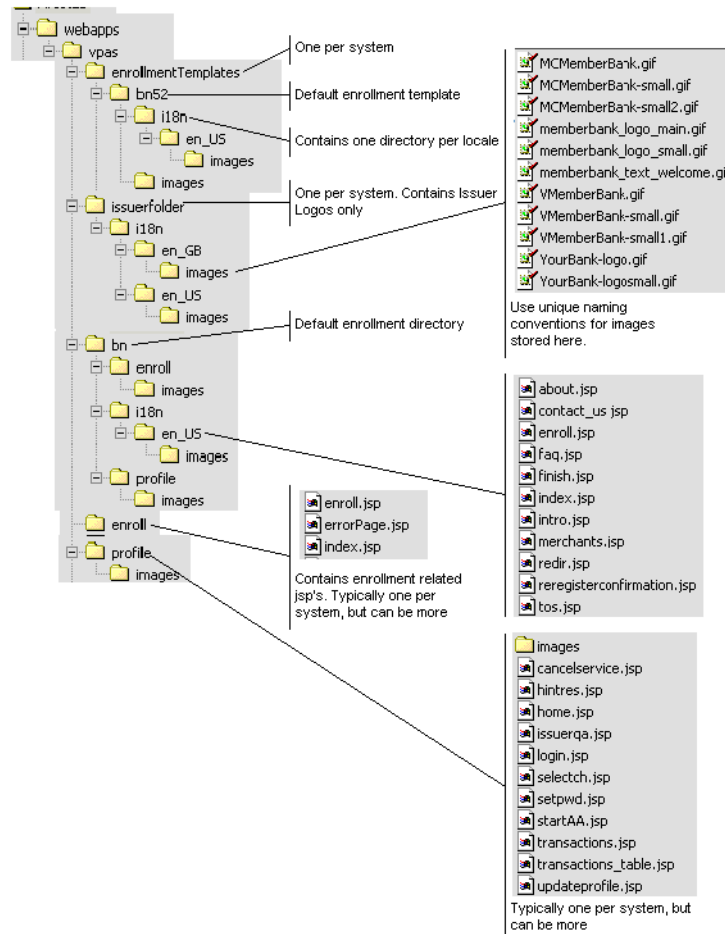
The customization process is described in the sections below:

Customizing the User Interface Template

The page layout data like the Issuer/range specific data is separated from the dynamic content from the UI. This ability allows you to design a template that is consistent in look and feel across the entire enrollment session. Multiple ranges can now share the same ES files, reducing the duplication of files per issuer.

The system by default supports two templates for MasterCard and Visa - called `sc` and `vbv` respectively. The ES templates use style-sheets which make customization easier. The templates are located in the

Root\$>: \CATALINA_HOME\webapps\vpas\enrollmentTemplates\ directory. You can create your own template based on the available templates and place in the same directory. To use the template you have created, use the [“Configuring Enrollment Process Attributes,”](#) link in the administrative console. See the [Figure 6-10 “ES Customization: Directory Structure,”](#) for more details.

Figure 6-10 ES Customization: Directory Structure

Customizing Enrollment Site text

The Enrollment site uses the following HTML and JSP files located in the `<$SystemRoot$>:\CATALINA_HOME\webapps\vpas\<seccode>\i18n\<locale>` directories:

Table 6-15 Enrollment site HTML and JSP files

File Name	Purpose
contact_us.html	Provides contact information for cardholder questions or concerns. This page appears when the cardholder clicks the Contact Us tab in the header menu.

Table 6-15 Enrollment site HTML and JSP files

File Name	Purpose
faq.html	Provides frequently asked questions and answers about the authentication service, shopping with the service, and enrolling in the service. This page appears when the cardholder clicks the FAQs tab in the header menu.
index.html	Acts as the home page for the Enrollment site.
tandc.html	Displays the Issuer's Terms and Conditions for the online authentication program. NOTE: The filename of any customized terms and conditions should be <code>tandc.html</code> .
finish.html	The last page of the enrollment process shown to the cardholder. Displays information about using 3-D Secure during purchase transactions.
forgotpassword.html	Displays information about the processes to follow if the cardholder forgets the secret password.
intro.html	The demo page giving a demonstration of how the online payment authentication program works.
merchants.html	Displays links to participating merchant sites and information on Issuer offers. This page appears when the cardholder clicks the Merchants & Offers tab in the header menu.
reg.html	Displays links to the standard enrollment and abridged enrollment pages.

Customizing Enrollment Site Graphics

Customizing ES Graphics for MasterCard Configurations

Replace the following GIF files with GIF files containing the applicable Issuer's branding logo or text:

- `logo_main.gif`
- `logo_small.gif`

These files are located in the `<$SystemRoot>\CATALINA_HOME\webapps\vpas\Issuer Folder\i18n\<locale>\images` directory.

The following are illustrations of each of these default GIF files along with size information:

Figure 6-11 logo_main.gif

Your Bank

Size: 180 x 90 (pixels), 8 bits per color channel

Figure 6-12 logo_small.gif

Your Bank

Size: 146 x 86 (pixels)

The logo_main.gif and logo_small.gif files appear in several different Enrollment site pages. The new customized file names should be provided through the [“Configuring Enrollment Process Attributes,”](#) link from the administrative console. When you provide the customized file names, all the pages will automatically display the customized graphics.

NOTE: While using the new ES, follow unique naming conventions for the image files in this folder. This folder is one per system and all the image files of the system should be stored here.

Customizing ES Graphics for Visa Configurations

Replace the following GIF files with GIF files containing the applicable Issuer's branding logo or text:

- logo_main.gif
- logo_small.gif
- text_welcome.gif

These files are located in the <\$System
Root\$>:\CATALINA_HOME\webapps\vpas\
Issuer Folder<Issuer Directory>\i18n\<locale>\images directory.

NOTE:

The file names of the customized files *must* be the same as the generic files, and they *must* be saved to the original directories.

The following are illustrations of each of these default GIF files along with size information:

Figure 6-13 logo_main.gifThe logo consists of the words "MEMBER BANK" in a blue, serif, all-caps font. The letters are widely spaced, giving it a clean, professional appearance.

Size: 120–180 x 20–90 (pixels), 8 bits per color channel
Recommended size is 140 x 47.

Figure 6-14 logo_small.gifThis is a smaller version of the "MEMBER BANK" logo, maintaining the same blue serif font and wide letter spacing.

Size: 124 x 20(pixels)

Figure 6-15 text_welcome.gifThe graphic displays the word "Welcome" in a large, black, serif font. Below it, in a smaller black serif font, are the lines "to MemberBank's" and "Verified by Visa Service!".

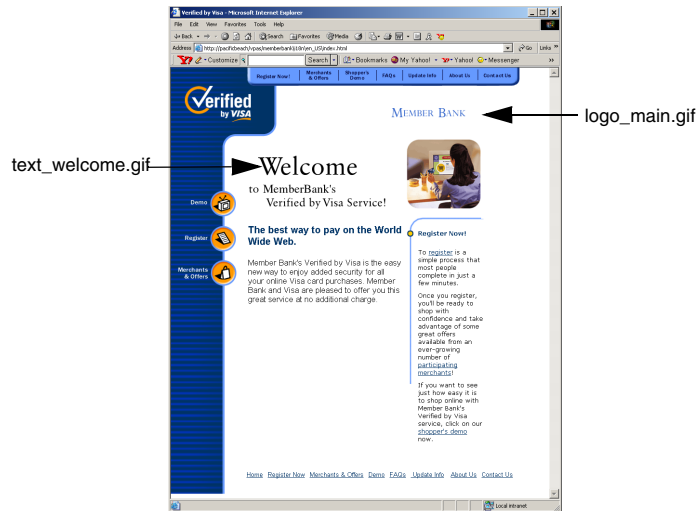
Size: 240–300 x 90–120 (pixels), 8 bits per channel, black font on white background
Font: Adobe Garamond

The logo_main.gif and logo_small.gif files appear in several different Enrollment site pages, while the text_welcome.gif only appears in the index.html page. When you replace these files with customized files with the same names, all pages will automatically display the customized graphics.

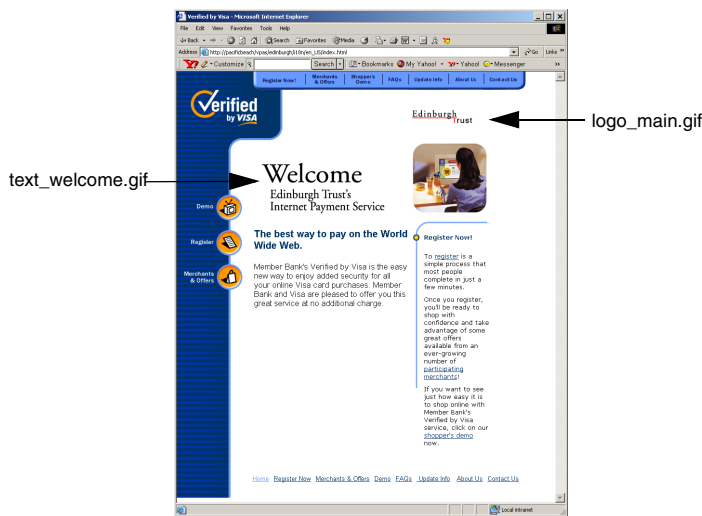
The logo_main.gif and logo_small.gif files appear in several different Enrollment site pages. The new customized file names should be provided through the “[Configuring Enrollment Process Attributes](#),” link from the administrative console. When you provide the customized file names, all the pages will automatically display the customized graphics.

NOTE: While using the new ES, follow unique naming conventions for the image files in this folder. This folder is one per system and all the image files of the system should be stored here.

For example, the generic logo_main.gif and text_welcome.gif files appear in the `..\<Issuer Directory>\i18n\<locale>\index.html` file (the Enrollment site start page) as follows:

Figure 6-16 ..index.html before customization

The following figure illustrates the `index.html` page after the `logo_main.gif` and `text_welcome.gif` files are customized:

Figure 6-17 index.html after customization

Customizing Message Files

There are two message files that are installed for each locale supported by the Issuer Software: `ErrorMessage.properties` and `StaticMessage.properties`. These files contain message text that appears on your Administrative Console (for Administrators and Issuer Administrators only).

All Issuer accounts may share these message files. However, if you want to customize the message text for a particular Issuer account, you must create new, Issuer-specific message files.

CAUTION:

If you change error messages, Issuer Software product support is compromised. If you need to edit the `ErrorMessage.properties` file, Arcot recommends that you consult with Arcot Professional Services.

To create an Issuer-specific message file:

1. Using the Windows Explorer, locate the following directory:

`<%System Root%>:\CATALINA_HOME\webapps\vpas\web-inf\classes`

2. Copy the applicable **`ErrorMessages_<language>_<country>.properties`** file and paste it into the same directory (in other words, into the `..\classes` directory).

NOTE:

The `ErrorMessages.properties` and `StaticMessages.properties` files are the files used for the `en_US` locale.

3. Rename the file as follows:

`ErrorMessages_<language>_<country>_<IssuerAccountDirectory>.properties`

For example:

`ErrorMessages_fr_FR_metrobank.properties`

4. Repeat steps 2 - 3 for the applicable `StaticMessages_<language>_<country>.properties` file, following the same naming convention.
5. Edit the messages files as desired and save the files.

Configuring Forgot Your Password in ES

The Issuer Software provides the *Forgot Your Password* to allow the cardholder to change the password. The cardholder can change the password either during purchase transactions or through the Issuer enrollment website because this feature is supported both in the enrollment server and the access control server.

Pre-Setup Tasks

The concept behind the Forgot Your Password (FYP) feature is to authenticate the cardholder using the available cardholder attributes and then allow the cardholder to reset the password. The Issuer can use the following available options to authenticate the cardholder:

- Hint/Response feature
- Re-Enrollment
- Reset the password by contacting the administrator

Configuring Hint/Response

The Hint/Response feature presents the cardholder with a hint and allows the cardholder to specify a response after a configurable number of failed authentication attempts. If the cardholder enters the correct response, the system authenticates the user.

The Hint/Response method to authenticate the cardholder will be successful if:

1. The Hint/Response feature is configured for the Issuer or card range. The [“Configuring Cardholder Password Policy,”](#) link under the **Enrollment Process Configurations** heading in the menu allows the Global administrator to configure the Secret Question/Answer feature.
2. The Hint question and response should be set by the cardholder or the data should be uploaded for pre-enrolled cardholders.
3. The maximum number of times the cardholder can attempt authentication using the Hint/Response feature can be controlled. A parameter called **Max Auth Tries** can be set in the [“Adding Financial Institution Information to the Issuer Account”](#) on page 85 screen.

Configuring Re-Enrollment

If the Hint/Response feature is not configured for the Issuer, you can alternately configure the Re-Enrollment feature to authenticate the cardholder when the password is reset at the Issuers enrollment website. The Issuer can ask questions to identify the cardholders. To authenticate the cardholder using this feature, the following tasks must be completed:

1. Configure the Issuer Q/A step during the standard enrollment process. See [“Configuring Order for Standard and Abridged Enrollment” on page 108](#) for more information.
2. The cardholder responses to the Issuer questions should be available for authentication. The responses can be uploaded into the database by using the Arcot Data Upload Tool for TransFort. See the *Arcot Data Upload Tool for Transfort Installation and User Manual* for more information on this utility.
3. Configure the *“Post Verification (Issuer QA) Step Callout,”* if the cardholder responses are not available in the Transfort database. To develop and configure CallOuts contact the Arcot Technical Support.

Resetting Cardholder Password from Issuer’s Enrollment Website

When the cardholder forgets the secret password or wants to change the password due to security reasons, the cardholder can reset or change the secret password from the *Account Assistant* link in the Issuer’s enrollment website. The Account Assistant requires the password to login. See the *Arcot TransFort Issuer Software Introduction Manual* for more details. The process flow is shown in [Figure 6-24 “FYP in ES - Process Flow”](#).

When the cardholder clicks on this link, the actions which follow are explained below:

1. If the Hint/Response for the password has been configured for the card range, and the Hint/Response information is available then the cardholder is shown the [“Hint/Response Page.”](#)

All the Hint questions for the card number are shown in a drop down box. The cardholder is asked to choose the hint question and provide the response in the text box. If the cardholder does not recognize any of the hint questions, there is an alternate link on the page which will go to the [“Re-Enrollment Page.”](#)

2. If the cardholder is authenticated using the response and the response identifies the cardholder, the cardholder is shown the [“Reset Password Page”](#). The cardholder can reset the password and is automatically logged into the Account Assistant.

3. If the cardholder is authenticated, but the response does not identify any particular cardholder for the given card number, then a drop down box with all the names for the card number is displayed and the cardholder is asked to choose a name. See [Figure 6-20 “Select Cardholder Page”](#).

The selected cardholder is shown the [“Reset Password Page.”](#) The cardholder can reset the password and is automatically logged into the Account Assistant.

4. If the Hint/Response feature is not enabled and if the Issuer Questions is configured for the card range, the cardholder is asked to enter the responses for the Issuer questions. See [Figure 6-19 “Re-Enrollment Page”](#).
5. If the cardholder is authenticated using the answers and the answers identifies the cardholder, the cardholder is shown the [“Reset Password Page”](#). The cardholder can reset the password and is automatically logged into the Account Assistant.
6. If the cardholder is authenticated, but the answers do not identify any particular cardholder for the given card number, then a drop down box with all the names for the card number is displayed and the cardholder is asked to choose a name. See [Figure 6-20 “Select Cardholder Page”](#).
7. The selected cardholder is shown the [“Reset Password Page”](#). The cardholder can reset the password and is automatically logged into the Account Assistant.
8. In both the Hint/Response and Re-enrollment case, if the cardholder reaches the maximum number of authentication attempts, the cardholder is not logged in the account assistant. The [“Authentication Failed Page”](#) displays an appropriate message and the cardholder is locked out.
9. If both the Hint/Response and Issuer questions are not configured for the range then the cardholder sees a page informing the cardholder to contact a Customer Support Representative (CSR) to reset the password ([Figure 6-22](#)). Alternatively, the page can also have a link to a form to be filled and submitted to the Issuer online.

Figure 6-18 Hint/Response Page

Welcome | Register Now | Account Assistant | **Forgot your Password?** | Contact Us | Help

Forgot your Password

Please select the hint question and then enter answer to your hint question. **Click cancel if you don't know any.**

* indicates required fields

Card Number 4012001011000037

Secret Question

Answer*

Figure 6-19 Re-Enrollment Page and Mothers maiden name: .

Verified by Visa - Microsoft Internet Explorer

VERIFIED by VISA MEMBER BANK

Forgot Your Password

If you have forgotten your password, you can reset your password by verifying your identity with the information below.

Last four digits of SSN:

Mothers maiden name:

Figure 6-20 Select Cardholder Page

The screenshot shows a web page titled "Select Cardholder Page". At the top, there is a navigation bar with links: "Welcome", "Register Now", "Account Assistant", "Forgot your Password?", "Contact Us", and "Help". Below the navigation bar, the page content includes the heading "Forgot your Password" and the instruction "Please select your name from the list or click cancel if your name is not present in the list." A note states "* indicates required fields". The form contains a label "Your Name as it appears on card*" followed by a dropdown menu currently displaying "JOHN SMITH". At the bottom of the form are two buttons: "CANCEL" and "SUBMIT".

Figure 6-21 Reset Password Page

The screenshot shows a web page titled "Reset Password Page". At the top, there is a navigation bar with links: "Welcome", "Register Now", "Account Assistant", "Forgot your Password?", "Contact Us", and "Help". Below the navigation bar, the page content includes the heading "Set your Password" and the instruction "Please enter you new password according to the policy set for you and then click submit." A note states "* indicates required fields". The form contains several fields: "Card Number" with the value "4012001011000037", "Your Name as it appears on card" with the value "JOHN SMITH", "Password*" with an empty text box, and "Confirm Password*" with an empty text box. Below the "Confirm Password*" field, there is a password policy note: "3-10 characters , atleast-1 alphabets , atleast-1 numeric .". At the bottom of the form are two buttons: "CANCEL" and "SUBMIT".

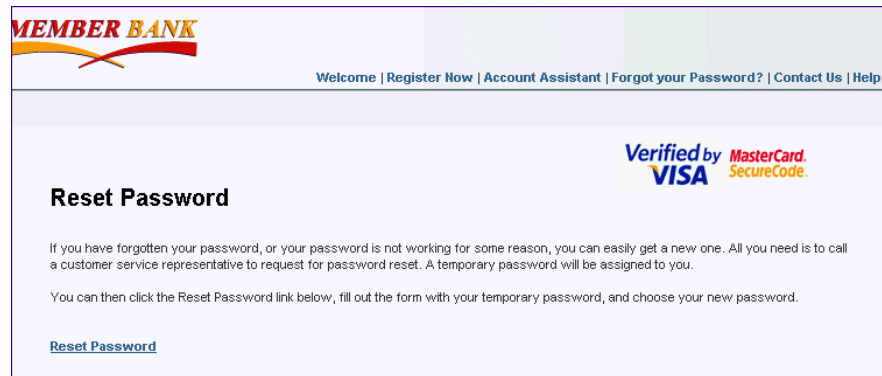
Figure 6-22 Contact CSR Page

Figure 6-23 Authentication Failed Page

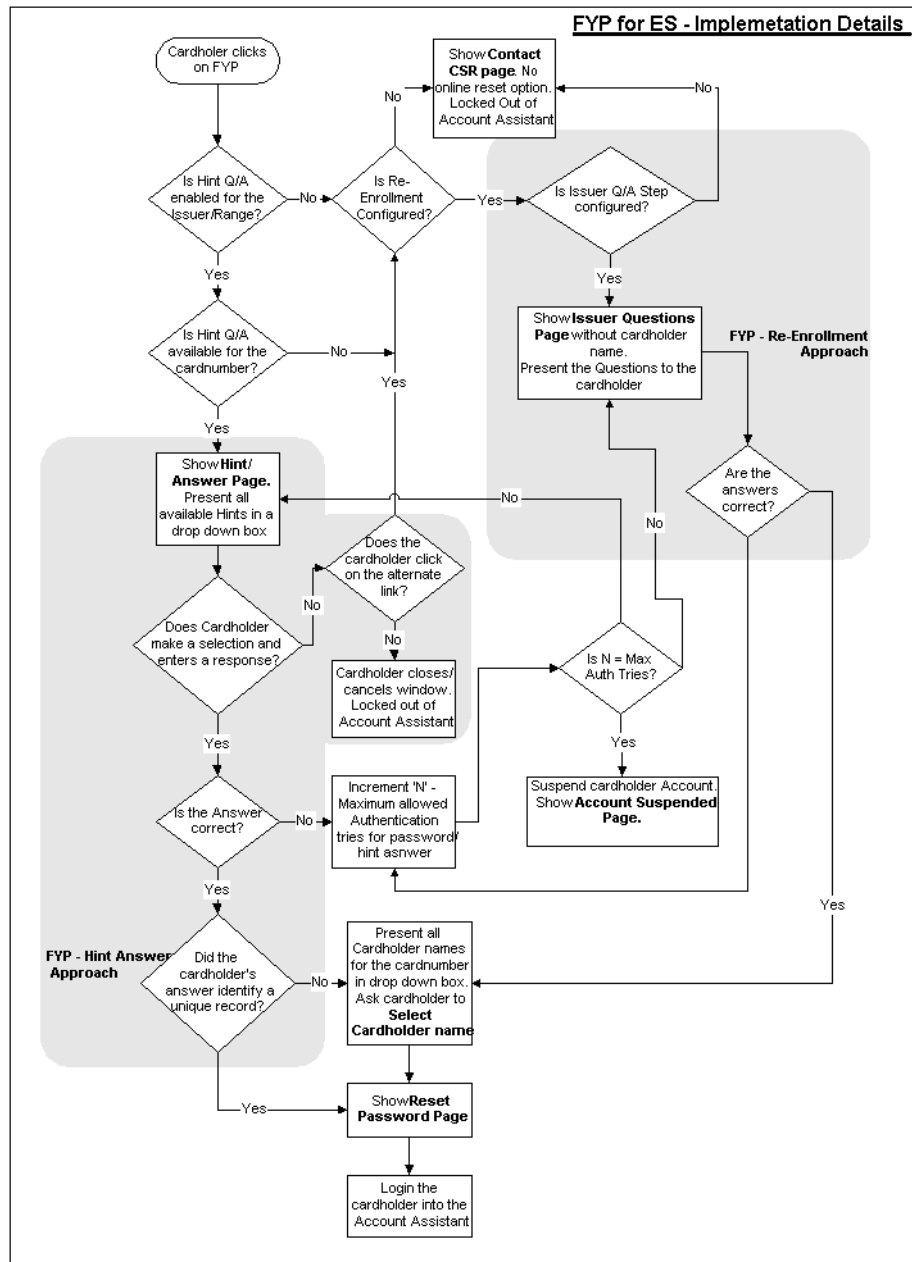
Welcome | Register Now | Account Assistant | **Forgot your Password?** | Contact Us

Account Assistant
Access a variety of features for quick and easy account management.

1. View the transaction history of online purchases made using your password.
2. Create a new password.
3. Edit your account profile.
4. Enroll another card.
5. Cancel your enrollment.

Log in	Learn More	Extras
<p>* indicates required fields Your account has been locked.</p> <p>User ID* <input type="text" value="JohnSmith"/></p> <p>OR</p> <p>Card Number* <input type="text"/></p> <p>Password* <input type="password"/></p> <p>Forgot your Password?</p> <p><input type="button" value="SUBMIT"/></p>	<p>Verified by VISA MasterCard SecureCode</p> <p>This is a place holder for Localized content from <enrollment folder>/18n/<locale>/index.jsp</p>	<p>This is a place holder for Localized content from <enrollment folder>/18n/<locale>/index.jsp</p>

[Welcome](#) | [Register Now](#) | [Account Assistant](#) | [Forgot your Password?](#) | [Contact Us](#)
[Help](#) | [Participating Merchants](#) | [About Us](#) | [Privacy Policy](#) | [Terms of Service](#)

Figure 6-24 FYP in ES - Process Flow

Chapter 7

Configuring the Access Control Server

The Issuer should configure the Access Control Server to authenticate the cardholders online transactions. The following sections describe the various tasks related to ACS configuration:

- Updating the ACS Configuration
- Adding Support for Mobile Device
- Adding Issuer Template Customization
- Customizing the Issuer's Client Authentication Pages
- Configuring Forgot Your Password in ACS

NOTE:

This tasks described in this chapter are privileges of a Global Administrator. Whether or not you have authority to complete the tasks described is defined by another Global Administrator or your Master Administrator.

Updating the Access Control Server Configuration

You can use the Administrative Console to globally configure certain parameters across all instances of the ACS you may have installed in your Issuer Software deployment. These parameters include HSM, Receipt Server, and AHS configuration.

Before you configure the ACS using the Administrative Console, you need to obtain the applicable AHS certificates. See [“Obtaining the AHS Certificates and Key” on page 144](#) for information.

To configure parameters for a particular instance of the ACS in your Issuer Software deployment, see [“ACS Configuration File \(acs.ini\)” in Chapter 9](#).

To update the Access Control Server Configuration:

1. Click the **Update ACS Config** link.

The *Update Access Control Server Configuration* page appears.

2. Update the applicable fields with the appropriate information.

The following table describes the fields on this page:

Table 7-1 Update Access Control Server Configuration fields

Field	Description
CVVKeyIndicator*	The configurable key indicator value used for CVV calculation. Default value is 01. See “Obtaining the CVV Key Indicator,” for more information.
Send Receipt	This parameter decides whether the system has to generate and send the transaction receipts to the receipt server. The possible values are: <ul style="list-style-type: none"> • 0 - Create, but don't send the receipts • 1 - Create and send the receipts
ReceiptQueueSize	The number of active receipts kept in the ACS Receipt Handler queue before being sent to the Receipt Server.
ReceiptWaitPeriod	The number of seconds the receipt dispatch thread will sleep between attempts to check the ACS receipt memory cache for new receipts. Default value is 10 seconds.
ReceiptServerWaitPeriod	The number of seconds between ACS to AHS connection attempts. Default value is 300 seconds.

Table 7-1 Update Access Control Server Configuration fields

Field	Description
ACSClusterId	The ACS cluster ID for receipts sent to the AHS.
AHSLoginId	The login ID for the ACS to use to access the AHS.
AHSPassword	The password associated with the AHSLoginId.
Profile	This parameter decides if you want the ACS debug profiling to be enabled. The possible values are: 0 - Debug profile off 1 - debug profile on
RingBufferSize	The number of transactions that can be cached in memory. Default value is 6000.
ACSDSRcvTimeout	The number of seconds that the ACS will wait for a request from the DS before the connection will be closed. Default value is 0, which indicates the ACS will fall back to underlying TCP timeout.
ACSAHSRcvTimeout	The number of seconds that the ACS will wait for a response from the AHS before the connection will be closed. Default value is 0, which indicates the ACS will fall back to underlying TCP timeout.
ACSAHSConnTimeout	The number of seconds that the ACS will wait to connect to the AHS before the connection will be timed out. Default value is 0, which indicates the ACS will fall back to underlying TCP timeout.
ACSAdminRcvTimeout	The number of seconds that the ACS will wait for a request on the Admin listener before the connection will be closed. Default value is 0, which indicates the ACS will fall back to underlying TCP timeout.
AHSCACertFile	The path and file name of the AHS Server CA Certificate. See “Obtaining the AHS Certificates and Key” on page 144 for more information.
AHSClientCertFile	The path and file name of the AHS Client SSL Certificate. See “Obtaining the AHS Certificates and Key” on page 144 for more information.
AHSClientKeyFile	The path and file name of the AHS Client SSL key. See “Obtaining the AHS Certificates and Key” on page 144 for more information.

Table 7-1 Update Access Control Server Configuration fields

Field	Description
CalloutConnPolicy	<p>The connection pooling policy to be used by the in-proc CallOut dll implementation. Currently two policies are supported.</p> <p>NoConnectionReuse - This policy means connections will not be reused. Effectively new connection is made for every CallOut request.</p> <p>OneReusableConnectionPerConfiguration - For every CallOut configuration one connection is maintained and CallOut to the same configuration will be serialized. This is the default policy.</p>
UseCVVWithXID*	<p>This parameter is specific to only version 1.0.1 of 3-D Secure. It sets the algorithm used by the PAREq's to calculate the CVV.</p> <p>If the value is 1, the algorithm used to calculate CVV is XID.</p> <p>if value is 0 the algorithm used is ATN.</p>
MaskPANinPAREs	<p>The parameter is specific to the 1.0.2 version of 3-D Secure. The parameter defines whether the PAREq should mask the PAN (last four digits).</p> <p>Set 1 to mask the PAN in the 1.0.2 PAREs</p> <p>Set 0 not to mask the PAN in the 1.0.2 PAREs.</p>
AllowAttemptsFor1_0_1	<p>This parameter indicates if the <i>Purchase Attempts</i> feature is supported for protocol 1.0.1.</p> <p>If the value is 1, the ACS supports Attempts for 1.0.1</p>
AETxnStatusInPaRes	<p>If the Attempts feature of ADS is supported for 1.0.1, then the transaction status code in the PaRes is set by this parameter. The valid values are Y or N or U.</p>
Default Folder	<p>The default folder to fall back when the CAP cannot locate the folder which is configured. The default is en_US.</p>
ProxyPanRetireTime	<p>The lifetime (in days) of the transaction ProxyPAN is limited to a fixed but configurable duration using this parameter. The default value is 90 days.</p> <p>NOTE: The transaction ProxyPAN cannot be really one-time over an extended period of time as the size of the ProxyPAN is restricted to a maximum of 28 bytes. Irrespective of the underlying algorithm used to generate this transaction ProxyPAN, it will repeat over time.</p>

Table 7-1 Update Access Control Server Configuration fields

Field	Description
HSM<N>DeviceName	<p>The crypto devices supported by the ACS. The devices supported are:</p> <ul style="list-style-type: none"> • nfast - the nCipher SSL accelerator to store the sensitive bank keys, signing keys, etc. • ibm4758 - the PKSCS11 interface of the IBM 4758 crypto card. • cca - the CCA interface of the IBM 4758 crypto card. • zaxus - the Thales HSM to store the CVV keys. <p>NOTE: You must to configure one of the devices from this field for the ACS to connect to the device.</p>
ACSCapRcvTimeout	The number of seconds that the ACS will wait for a request from the CAP before the connection will be closed. Default value is 0, which indicates the ACS will fall back to underlying TCP timeout.

- When you have completed updating the applicable fields, click **Submit**.
The message “ACS configuration parameters updated” appears.
- Run `ACSCliant` to refresh the ACS table cache. See “[Refreshing ACS Cache](#)” in [Chapter 10](#) for detailed instructions.

Figure 7-1 Update ACS Configuration Page

Update Access Control Server Configuration	
Configure the appropriate values for the various attributes of the Access Control Server and click Save to save the configuration. Click Refresh to refresh the cache.	
CVWKeyIndicator	01
ReceiptQueueSize	100
ReceiptServerWaitPeriod	300
AHSLoginId	
Profile	1
ACSDSRcvTimeout	0
ACSAHSConnTimeout	0
AHSACertFile	C:/Program Files/Common
AHSClientKeyFile	C:/Program Files/Common
UseCVWWithXID	0
AllowAttemptsFor1_0_1	0
DefaultFolder	en_US
ACSCapRcvTimeout	0
SendReceipt	1
ReceiptWaitPeriod	120
ACSClusterId	
AHSPassword	
RingBufferSize	6000
ACSAHSRcvTimeout	0
ACSAdminRcvTimeout	0
AHSClientCertFile	C:/Program Files/
CalloutConnPolicy	OneReusableConn
MaskPANinPARES	1
AETxnStatusInPaRes	U
ProxyPanRetireTime	90
LogPATransReq	1

Obtaining the AHS Certificates and Key

You need to obtain and install the following certificates and key, which are required for communication between the ACS and the AHS:

- AHS Server CA Certificate
- Client SSL Certificate
- Client SSL Private Key

All files must be in PEM format.

When you have obtained these items, do the following:

1. Concatenate the Client SSL Certificate and the Client SSL Private Key into a single file.
2. Copy the files to the following location:

```
<$System Root$>:\Program Files\Common Files\Arcot Shared\ssl
```

See [Appendix D, “Certificates Required](#) for more information regarding the certificates required for the TransPort Issuer Software system.

Adding Support for Mobile Device

This function allows you to add support for different mobile phones that may be used by your cardholders. Please contact Arcot Systems for more information before attempting to perform this function.

To add support for a mobile phone:

1. Click the **Add New Phone Support** link.

The *Add New Phone Support* page appears.

2. Type the applicable information in the appropriate fields.

The following table lists the fields on this page and provides descriptions of each:.

Table 7-2 Add New Phone Support page fields

Field	Description
User Agent	An HTTP user agent that supports mobile device authentication.
Accept String	An HTTP accept string that supports mobile device authentication.
Content Type	Specifies the content type of the accept string.

3. Click **Submit**.

The message “Support for new phone added” appears.

Adding Issuer Template Customization

The GIF, HTML, and certain JavaScript files used in the cardholder password pages during a purchase transaction are installed to the

For windows:

- <\$System Root\$>:\inetpub\wwwroot\acspage\<locale>\

For Unix:

- /opt/arcot/CAP/acspage/<locale>

All Issuer accounts can share these files. The [Table 7-3](#) lists and describes all the files in this directory. However, if you want to customize these files for a particular Issuer or for a particular card range (for example, to add a branding logo), you need to create a subdirectory to . . \acspage for the Issuer and then define the subdirectory in the Issuer Software.

Table 7-3 CAP files

CAP filename	Description
AcctDisabled.htm	This file is displayed when the cardholder status is locked. The cardholder can be locked from the system due to authentication failure during regular authentication, FYP or ADS.
arcqrtn.htm	This page is displayed when the cardholder completes a chip card transaction.
askchnamebase.htm	This page allows the cardholder to select a name. During FYP, when the cardholder's responses match multiple cardholders, the cardholder is asked to select a name.
attempts.htm	The page displayed for the ranges which are configured for Attempts form of ADS.
chiphelp.htm	Help page for the chip card transaction.
conditions.htm	The page displays the conditions for use of service.
getemail.htm	The pop under page during attempts/decline transaction that is shown to the cardholders asking for their email.
help.htm	This page displays the help during transactions. The link to this page is in the password page.
hintbase.htm	The Hint Question and answer page displayed during FYP.
hinhelp.htm	Help for the hint page.

Table 7-3 CAP files

CAP filename	Description
hrtabase.htm	This page is displayed when the cardholder fails authentication using hint/response. The cardholder can also see this page when, <ul style="list-style-type: none"> the bank is not configured to lock the cardholder after 'N' strikes and the range is not configured for hint/answer
multipwdbase.htm	The page is used to collect the cardholder password during ADS. The page is also displayed when the cardholder resets password using the FYP functionality.
optin.htm	Opt-in page, asking the user if they want to join the online authentication program now or later. Also used when the user clicks on “ Forgot your password? ” link and the VIA callout is configured.
optindecline.htm	This page pops up when the cardholder declines to join the program.
postauth.htm	A Thank You page displayed during ADS after the transaction is completed.
pwdbase.htm	The page asks for the enrolled cardholder to enter the password for authentication.
pwdhint.htm	This page is displayed when the cardholder clicks on the “ <i>Forgot Your Password</i> ” link. This page is also shown to the cardholder only when there is no other way of authenticating the cardholder - No VIA callout as well or Hint question and answer.
rtnbase.htm	Is used when the transaction is complete and PAREs is being sent.
submitToES.htm	This page contains the URL to the ES, where the request for mini enrollment should be posted to.
terms.htm	Purchase terms
welcome.htm	Welcome page after the cardholder has joined the program using ADS, provided the Maxwelcome is > NumWelcome for the cardholder.

For information on how to customize the password pages, see “[Customizing the Issuer’s Client Authentication Pages](#)”.

To create the Issuer Template subdirectory:

1. Using the Windows Explorer, locate the acspage following directory:

2. Create a new subdirectory under the `..\acspage` directory. For example `metrobank_en_US`.
3. Copy the entire directory of the locale you wish to customize. Paste it into the new subdirectory. (in other words, into the `..\acspage\metrobank_en_US` directory).
4. Customize the files under the new subdirectory as desired and save them.
5. Repeat the steps 1 to 4 for all the locales you want to customize.

To define the customized templates in the Issuer Software:

1. In the Administrative Console, click the **Add Issuer Customization** link.

The *Customize ACS-CAP Template* page appears.

2. Enter the applicable data in the appropriate fields.

The following table provides descriptions of the fields on this page:

Table 7-4 Add Issuer Customization fields

Fields	Description
Issuer Name	The Issuer account for whom you are adding customized templates.
Card Range	The available card ranges or the range group for the selected Issuer for which you may add ACS-CAP customization. Select a card range from the drop-down box.
Locale	The Issuer locale for which you are adding customized templates.
Device Category	The user's device type for which the templates were customized. Options are: PC—Desktop computer Mobile—Mobile device
User Agent	If Mobile is selected, the user agent supporting authentication (for example, phone browser type).
Accept String	If Mobile is selected, the string supporting authentication (for example, WML).
ACS-CAP Folder Name	The name of the subdirectory you created to hold the Issuer-specific customized templates for the selected locale (for example, <code>metrobank_en_US</code>).

3. Click **Submit**.

The message “Issuer Customization added/updated” appears.

Customizing the Issuer's Client Authentication Pages

The GIF, HTML, and certain JavaScript files used in the Client Authentication Pages (CAP) user interface during a purchase transaction are installed to the `<$SystemRoot$>:\Inetpub\wwwroot\acspage` directory according to locale. Although you may customize these files as desired, there are only two GIF files that require customization for an Issuer. Otherwise, the password page files are ready to use.

This section provides information on customizing the CAP GIF files. If you would like to extensively customize the password pages, for example for mobile phone use, please contact Arcot Systems for more information.

Before customizing any of these files, you need to create an Issuer directory for customized CAP files. When you have completed customizing the files, you need to define the directory for the Issuer in the Issuer Software. For detailed instructions, see [“Adding Issuer Template Customization”](#).

For information on how to set the title of the password popup page, see [“CAP Configuration File \(cap.ini\)”](#) in [Chapter 9](#).

Customizing the CAP Graphics

The following two GIF files should be replaced with the Issuer's branding logo or text:

- BankLogo.gif
- member_logo.gif

These files are located in the `<$SystemRoot$>:\Inetpub\wwwroot\acspage\<locale>\images` directories.

NOTE:

The file names and graphic sizes of the customized files *must* be the same as the generic files, and they *must* be saved to the original directories.

The following are illustrations of each of these generic GIF files along with graphic size information:

Figure 7-2 BankLogo.gif



FIRST USA

Size: 104 x 32 (pixels)

Figure 7-3 member_logo.gif



MEMBER BANK

Maximum size: 140 x 47 (pixels).

The image must be static - not animated. For optimal screen load time, the image file size should not exceed 5 KB.

The `member_logo.gif` image is displayed on many of the password pages while the `BankLogo.gif` image is only displayed on the `hinthelp.htm` page.

Configuring Forgot Your Password in ACS

The Issuer Software provides the *Forgot Your Password* to allow the cardholder to change the password. The cardholder can change the password either during purchase transactions or through the Issuer enrollment website because this feature is supported both in the enrollment server and the access control server.

You can enable the FYP feature automatically to ensure the cardholder is presented with the FYP options instead of waiting for the cardholder to click on the FYP link provided. See [“Auto FYP,”](#) for more details.

Pre-Setup Tasks

The concept behind the Forgot Your Password (FYP) feature is to authenticate the cardholder using the available cardholder attributes and then allow the cardholder to reset the password. The Issuer can use the following available options to authenticate the cardholder:

- Hint/Response feature
- Re-Enrollment
- Reset the password by contacting the administrator

Configuring Hint/Response

The Hint/Response feature presents the cardholder with a hint and allows the cardholder to specify a response after a configurable number of failed authentication attempts. If the cardholder enters the correct response, the system authenticates the user.

The Hint/Response method to authenticate the cardholder will be successful if:

1. The Hint/Response feature is configured for the Issuer or card range. The [“Configuring Cardholder Password Policy,”](#) link under the **Enrollment Process Configurations** heading in the menu allows the Global administrator to configure the Secret Question/Answer feature.
2. The Hint question and response should be set by the cardholder or the data should be uploaded for pre-enrolled cardholders.
3. The maximum number of times the cardholder can attempt authentication using the Hint/Response feature can be controlled. A parameter called **Max Auth Tries** can be set in the [“Adding Financial Institution Information to the Issuer Account”](#) on [page 85](#) screen.

Configuring Re-Enrollment

If the Hint/Response feature is not configured for the Issuer, you can alternately configure the Re-Enrollment feature to authenticate the cardholder when the password is reset at the Issuers enrollment website. The Issuer can ask questions to identify the cardholders. To authenticate the cardholder using this feature, the following tasks must be completed:

1. Configure the Issuer Q/A step during the standard enrollment process. See [“Configuring Order for Standard and Abridged Enrollment” on page 108](#) for more information.
2. The cardholder responses to the Issuer questions should be available for authentication. The responses can be uploaded into the database by using the Arcot Data Upload Tool for TransFort. See the *Arcot Data Upload Tool for Transfort Installation and User Manual* for more information on this utility.
3. Configure the *“Verify Issuer Answers,”* if the cardholder responses are not available in the Transfort database. To develop and configure CallOuts contact the Arcot Technical Support.

Resetting Cardholder Password from Issuer’s Enrollment Website

When shopping at a participating merchant’s website, the cardholder clicks Buy, the password page pops-up. At this point the cardholder has to enter the password to complete the purchase. If a cardholder has forgotten the password, the “Forgot Your Password” link on the page ([Figure 7-4](#)) will enable the cardholder to reset the password. The process flow is shown in [Figure 7-11 “FYP in ACS - Process Flow”](#).

When the cardholder clicks on this link, the actions which follow are explained below:

1. If the Hint/Response for the password has been configured for the card range, and the Hint/Response information is available then the cardholder is shown the [“Hint/Response page.”](#)

All the Hint questions for the card number are shown in a drop down box. The cardholder is asked to choose the hint question and provide the response in the text box. If the cardholder does not recognize any of the hint questions, there is an alternate link on the page which will go to the [“Re-Enrollment Page”](#).

2. If the cardholder is authenticated using the response and the response identifies the cardholder, the cardholder is shown the [“Reset Password Page.”](#) The cardholder can reset the password and the purchase transaction is authenticated.

3. If the cardholder is authenticated, but the response does not identify any particular cardholder for the given card number, then a drop down box with all the names for the card number is displayed and the cardholder is asked to choose a name. See [Figure 7-10 “Select Cardholder Account Page”](#).

The selected cardholder is shown the “[Reset Password Page](#).” The cardholder can reset the password and the purchase transaction is authenticated.

4. If the Hint/Response feature is not enabled and if Re-enrollment is configured for the card range, the cardholder is asked to enter the responses for the questions. See [Figure 7-6 “Re-Enrollment Page”](#).
5. If the cardholder is authenticated using the answers and the answers identifies the cardholder, the cardholder is shown the “[Reset Password Page](#).” The cardholder can reset the password and the purchase transaction is authenticated.
6. If the cardholder is authenticated, but the answers do not identify any particular cardholder for the given card number, then a drop down box with all the names for the card number is displayed and the cardholder is asked to choose a name. See [Figure 7-10 “Select Cardholder Account Page”](#).

The selected cardholder is shown the “[Reset Password Page](#).” The cardholder can reset the password and the purchase transaction is authenticated.

7. In both the Hint/Response and Re-enrollment case, if the cardholder reaches the maximum number of authentication attempts, the cardholder is shown the “[Authentication Failed](#)” and is locked out.
8. If both the Hint/Response and Re-enrollment are not configured for the range then the cardholder sees “[Contact CSR page](#)” informing the cardholder to contact a Customer Support Representative (CSR) to reset the password. Alternatively, the page can also have a link to a form to be filled and submitted to the Issuer online.

Auto FYP

The Forgot Your Password feature is enabled only when the cardholder clicks on the *Forgot Your Password* link. The cardholders who don't click on this link typically fail the transaction and also get locked. The Auto FYP is a feature where the FYP is automatically enabled once the cardholder fails authentication for a pre-configured number of attempts. The “[Max Auth Tries for Auto FYP](#),” field in the “[Adding Financial Institution Information to the Issuer Account](#),” section describes how to configure Auto FYP.

IMPORTANT:

You should make sure the number after which the Auto FYP feature is enabled (M) is smaller than the maximum number of authentication attempts (N), (Make sure always $M < N$).

Auto FYP has a process flow similar to the FYP feature described above.

Figure 7-4 Forgot Your Password Link during Purchase Transactions

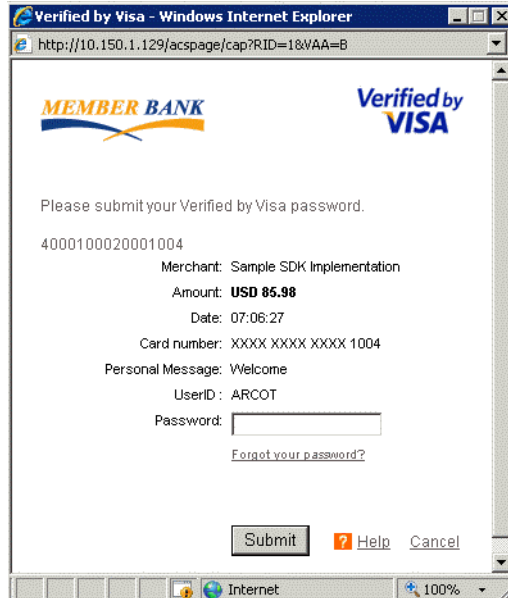


Figure 7-5 Hint/Response page

Verified by Visa - Microsoft Internet Explorer

MEMBER BANK **Verified by VISA**

Forgot Your Password

Secret Questions and Answers have been configured for this card. If one of the following questions belongs to you and you provide the correct answer, you will be able to reset your password immediately and complete this transaction.

Secret Question: **Birth Place**

Answer:

[Back](#) [? Help](#) [Cancel](#)

Note: If you cannot remember the answer to your Secret Question or are an additional cardholder on this account that has not configured a Secret Question, [click here](#) for information on resetting your password.

Internet

Figure 7-6 Re-Enrollment Page

Verified by Visa - Microsoft Internet Explorer

MEMBER BANK **Verified by VISA**

Forgot Your Password

If you have forgotten your password, you can reset your password by verifying your identity with the information below.

Last four digits of SSN:

Mothers maiden name:

Select Locale:

[Back](#)

Done Internet

Figure 7-7 Reset Password Page

Verified by Visa - Windows Internet Explorer

http://10.150.1.129/acspage/cap?RID=1&VAA=B

MEMBER BANK **Verified by VISA**

Reset Your Password

To reset your password, enter your password in the input boxes. Record your password in a safe place - It will be used on all future purchases at participating stores.

UserID : ARCOT

Enter Password

Re-enter Password

Receive Promotional Emails : ☐

[? Help](#) [Cancel](#)

Figure 7-8 Contact CSR page

Verified by Visa - Microsoft Internet Explorer

MEMBER BANK **Verified by VISA**

[? Help](#)

If you established a secret question when you registered for Verified by Visa then the correct answer to that secret question should be entered in the answer field. If you don't see a secret question, or if the secret question doesn't help you, you'll need to contact your customer service for additional help.

If you have specific questions about an account, please refer to the your customer service telephone number listed on your monthly billing statement.

[Return to password entry screen](#)

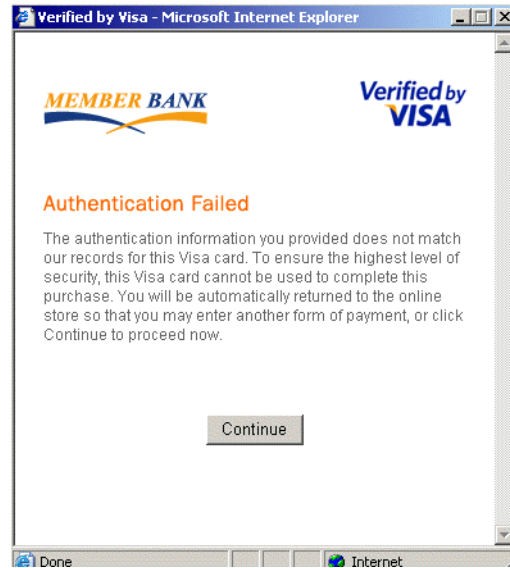
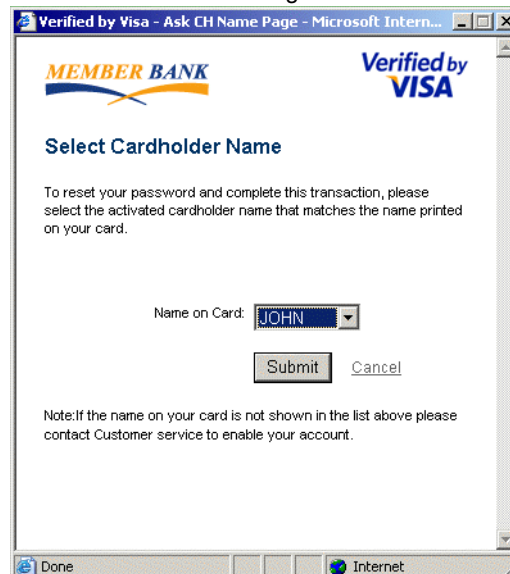
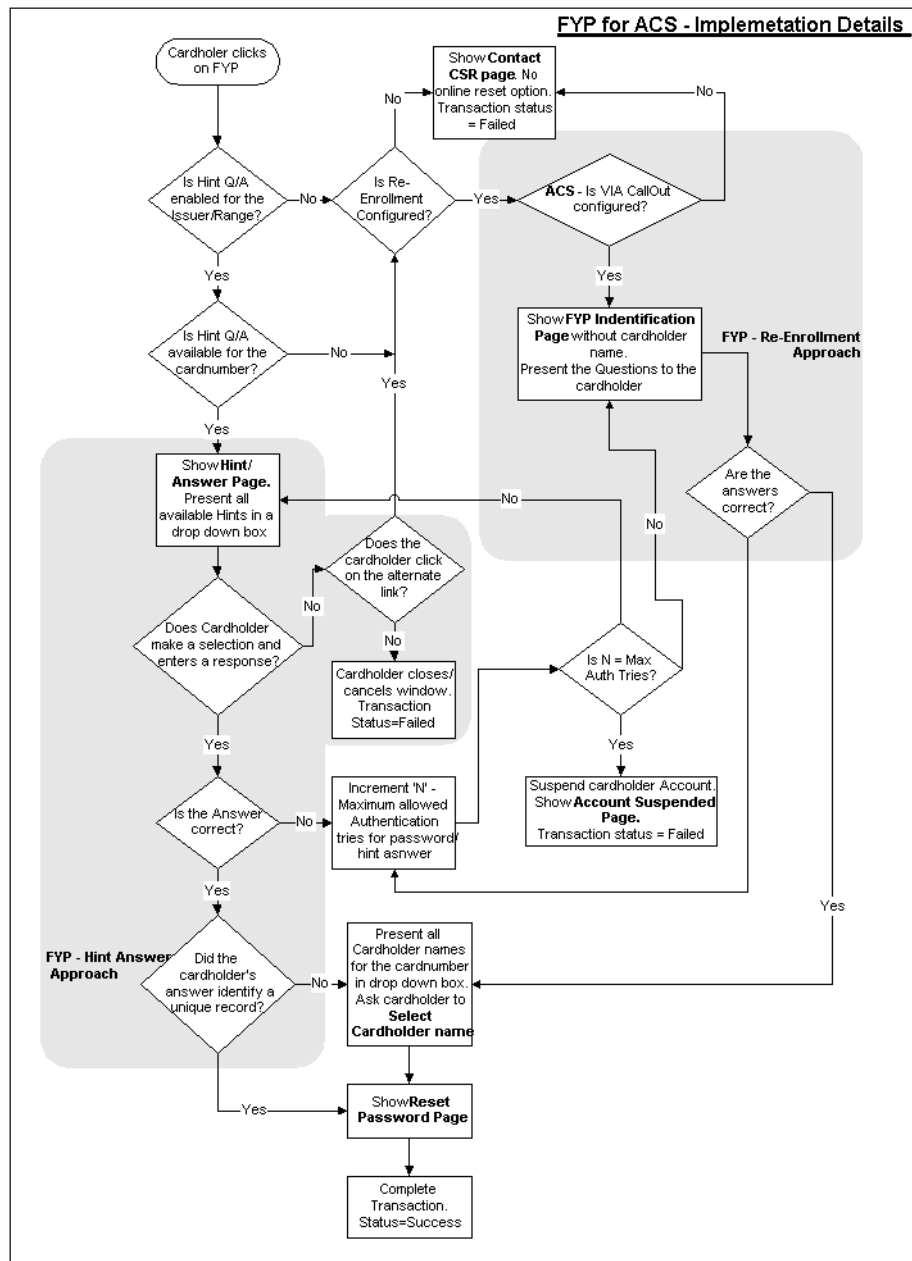
Figure 7-9 Authentication Failed**Figure 7-10 Select Cardholder Account Page**

Figure 7-11 FYP in ACS - Process Flow

Chapter 8

Configuring ADS

An Issuer can automatically enroll cardholders into the authentication program. This is achieved by introducing the cardholder to the virtues of the online payer authentication program while the cardholder is making a purchase on the Internet. This chapter describes the different ADS options available and how to configure ADS.

WARNING

The Issuer must ensure that the data collected cardholders during ADS must be the same as the data collected during standard enrollment.

Issuers can configure ADS in three methods:

- Opt-In Method
- Issuer Activation Method
- Purchase Attempts Method

These methods are described in detail in the sections below.

Configuring Opt-In

In this method the cardholder is introduced to the online payer authentication program while purchasing at a participating merchant's web site. The introduction to the authentication program is done through the *Opt-In* page. The cardholder can opt to activate through this page. When the cardholder decides to activate, the *Password* page to the online payer authentication program is shown. See the *Arcot TransFort Issuer Software Introduction Manual* for more information about the end user experience.

The following process flow diagrams describes the working of the Opt-In method of ADS in detail:

- [Optin - Using existing password.](#)
- [Optin - creating new password](#)
- [Optin - Decline](#)

The following tasks are required to configure the Opt-In method of AE:

1. Configuring the ADS parameters
2. Data Upload
3. Configuring CallOuts
4. Setting the PAREs Status
5. Changing the ES URL

Configuring the ADS parameters

The Issuer can configure the Opt-In method of enrollment with the following parameters. These parameters are configured via the administrative console. See “[Adding Financial Institution Information to the Issuer Account](#),” for more details.

Table 8-1 ADS Parameters

Parameter	Description
ADS Option	<p>The ADS Option for OptIn method are:</p> <ul style="list-style-type: none"> • <i>Opt-In - Cardholder uploaded</i> • <i>Opt-In - Cardholder not Uploaded</i>

Table 8-1 ADS Parameters

Parameter	Description
Max Decline	The number of times the cardholder can defer to Opt-In the online authentication program. The Global Administrator must define Max Decline as a value greater than 0.
Max Welcome	This parameter indicates the number of times a recently activated shopper (via ADS) will be informed about the online payer authentication program (with an optional hint to the password). Set Max Welcome to a value greater than 0.

Data Upload

If the ADS **Option** is set to **Opt-In - Cardholder Uploaded**, the Issuer should be upload the cardholder data in the database.

- The Issuer prepares a batch file of all required data elements for cardholder records, including passwords and personal messages used by the ACS.
- The file is uploaded using the Arcot Data Upload Tool and an account holder entry is created in the Issuer Software Database for each uploaded cardholder record.
- The Issuer communicates to cardholders that they have been pre-enrolled and communicates the cardholder's password and personal message to the cardholder.

Configuring CallOuts

If the ADS **Option** is set to **Opt-In Cardholder not Uploaded**, the Issuer should configure CallOuts to enable ADS. See *Arcot TransFort Issuer Software Introduction Manual* for more information.

- A CallOut can be specified for a verify password event if the cardholder password is not uploaded.
- A CallOut can be specified for the verify hint response event if the cardholder hint response is not uploaded or enabled.
- A CallOut can be specified for the Verify Issuer Answers event if the cardholder's responses to Issuer questions has to be authenticated.

Setting the PAREs Status

The PAREs status for 3-D Secure 1.0.1 during ADS can be set to U or N or Y. The default is 'U'. This parameter is set by the `AETxnStatusInPaRes` field in the *ACSConfig Page* in the administrative console.

Changing ES URL

The ES URL should be changed to the current ES URL in files under the CAP template files. The files are:

- `getemail.htm` (for cardholder email collection).

Enrolling Secondary Cardholder during ADS

During ADS the Issuer can enroll a secondary cardholder for the same card number. The page shown to the cardholder (see [Figure 8-7](#)) has a link [Add Sec CH](#) which takes the cardholder to the [Optin with Issuer Questions page](#).

The secondary cardholder is authenticated based on the responses to the Issuer questions and is allowed to set the secret password required to complete the online transactions.

NOTE: The feature to enroll the secondary cardholder is not available by default. Please contact Arcot Professional Services to customize this feature.

To ensure the secondary cardholder is enrolled successfully the Issuer has to complete the following tasks:

- The *Issuer Questions* and *Question Policy* is configured to enable enrollment of the secondary cardholder. See [“Configuring the Enrollment Process” on page 105](#) for more information.
- The responses of the cardholder should be uploaded to the Transfort database or the ACS CallOut - *Verify Issuer Answers* should be configured.

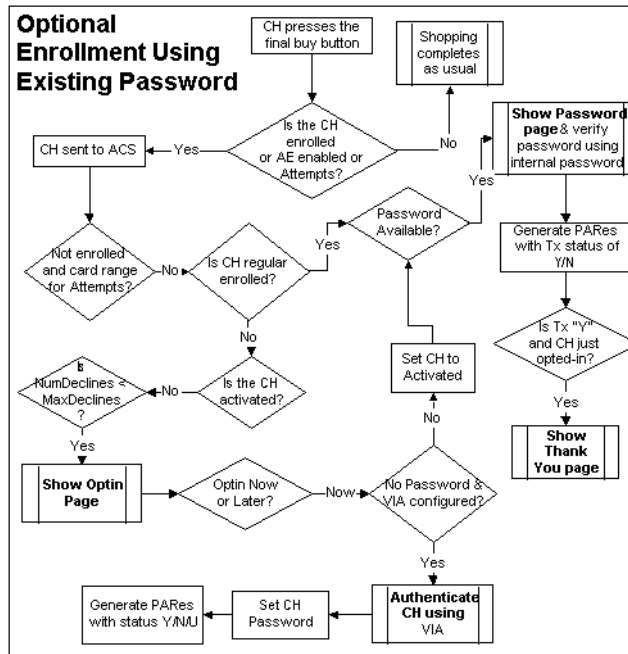
Figure 8-1 Optin - Using existing password.

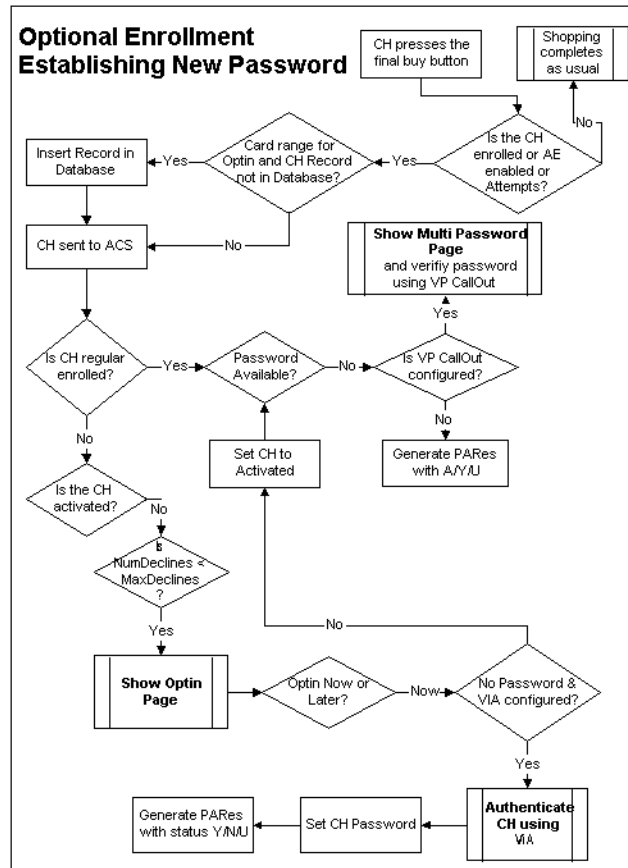
Figure 8-2 Optin - creating new password

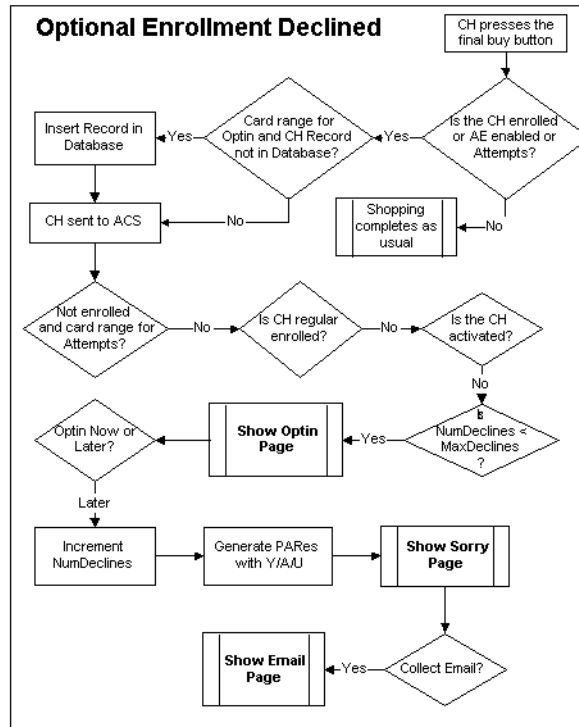
Figure 8-3 Optin - Decline

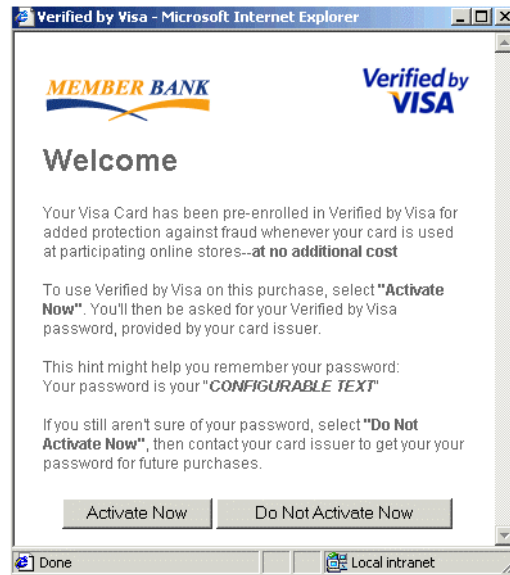
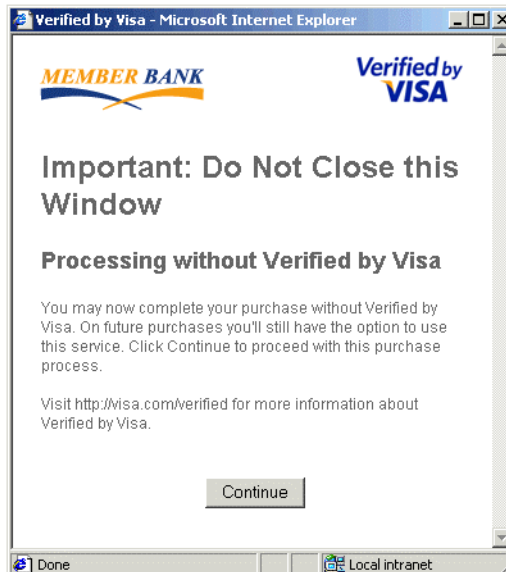
Figure 8-4 OptIn Page**Figure 8-5** Continue without Authenticating Transaction Page

Figure 8-6 Optin with Issuer Questions page

Verified by Visa - Windows Internet Explorer

http://10.150.1.129/acspage/cap?RID=1&VAA=A

MEMBER BANK **Verified by VISA**

Protect Your Visa Card Online

Your Visa Card has been pre-enrolled in Verified by Visa for added protection against fraud whenever your card is used at participating online stores--at **no additional cost**.

Merchant: Sample SDK Implementation
 Amount: **USD 46.99**
 Card number: XXXX XXXX XXXX 1004
 Personal Message: Welcome

Last four digits of SSN:
 Mothers maiden name:

Select Locale:

Figure 8-7 Add secondary Cardholder option

Verified by Visa - Windows Internet Explorer

http://10.150.1.129/acspage/cap?RID=1&VAA=B

MEMBER BANK **Verified by VISA**

Welcome to VBV

The Verified by Visa authentication system provides enhanced security for online purchases by authenticating the identity of the cardholder before purchase approval.

You may know more about the VBV program at:

"http://visa.com/verified"

Configuring Issuer Activation

The Issuer can upload cardholder data and pre-activate the cardholders. This is called *Issuer Activation*. The cardholder will be shown the “[Welcome Page](#),” directly. See the *Arcot TransFort Issuer Software Introduction Manual* for more information.

The [Issuer Activation](#) process flow diagram describes the working of the Issuer Activation method of ADS in detail.

The following tasks are required to configure the Issuer Activation method of AE:

- [Configuring the ADS parameters](#)
- [Data Upload](#)
- [Configuring CallOuts](#)

Configuring the ADS parameters

The Issuer can configure the Issuer Activation method of ADS with the following parameters. These parameters are configured via the administrative console. See “[Adding Financial Institution Information to the Issuer Account](#),” for more details.

Table 8-2 ADS Parameters

Parameter	Description
ADS Option	<p>The ADS Option for Issuer Activation method are:</p> <ul style="list-style-type: none"> • <i>Issuer Activation - Cardholder uploaded</i> • <i>Issuer Activation - Cardholder not Uploaded</i>
Max Decline	The number of times the cardholder can defer to Opt-In the online authentication program. The Global Administrator must define Max Decline = 0.
Max Welcome	This parameter indicates the number of times a recently activated shopper (via Auto-Enrollment) will be informed about the online payer authentication program (with an optional hint to the password). Max Welcome must be > 0.

Data Upload

If the ADS **Option** is set to **Issuer Activation - Cardholder Uploaded**, the Issuer should be upload the cardholder data in the database.

- The Issuer prepares a batch file of all required data elements for cardholder records, including passwords and personal messages used by the ACS.
- The file is uploaded using the Arcot Data Upload Tool and an account holder entry is created in the Issuer Software Database for each uploaded cardholder record.
- The Issuer communicates to cardholders that they have been pre-enrolled and communicates the cardholder's password and personal message to the cardholder.

Configuring CallOuts

If the ADS **Option** is set to **Issuer Activation Cardholder not Uploaded**, the Issuer should configure CallOuts to enable ADS. See *Arcot TransFort Issuer Software Introduction Manual* for more information.

- A CallOut can be specified for a verify password event if the cardholder password is not uploaded.
- A CallOut can be specified for the verify hint response event if the cardholder hint response is not uploaded or enabled.
- A CallOut can be specified for the Verify Issuer Answers event if the cardholder's responses to Issuer questions has to be authenticated.
- If the cardholder password is not available in the database and the VIA CallOut is not specified, and if the Verify Password CallOut is specified, the password page is shown. The cardholder is authenticated through the VP CallOut and the password is inserted in the database. See the “**Optin - creating new password**” flowchart for the process flow.

Adaptive ADS

The Opt-In and Issuer Activation ADS configurations described in the sections above work at a card range level. Once configured, the same set of rules applies to all transactions for the range. Adaptive ADS can change the rules based on transaction data. The ability to dynamically change the behavior of ADS based on transaction data is termed as “Adaptive ADS”. The process flow changes to follow Issuer Activation form of ADS and the users are mandated to enroll. For example, a cardholder can be “Issuer Activated” even if the range is configured for Opt-In ADS, based on the merchant data.

The Adaptive ADS behavior can be used for fraud prevention, improving merchant adoption and increasing transaction success rates. See the *Arcot TransFort Issuer Software Introduction Manual* for more information or contact Arcot Professional Services Group if you require Adaptive ADS.

IMPORTANT:

When you want to configure Adaptive ADS it is assumed that the range is already configured for either Opt-in or Issuer Activation form of ADS.

To configure a range or a range group for Adaptive ADS:

1. Click the **Adaptive ADS Configuration** link in the administrative console.

The Adaptive ADS Configuration page appears.

2. Select the Issuer to be configured and the appropriate card range or the range group to be configured for the Issuer and press **Submit**.

See “[Configuring for a Specific Range or Range Group](#),” for more details.

3. The Adaptive ADS Configuration page is displayed.

If you are configuring the Adaptive ADS rules for the first time, the system displays a message, “*No rules have been defined for this bank and range.*” Otherwise the fields display the existing rules for the range selected.

4. Currently the Adaptive ADS rules are based on:
 - a. Merchant IDs
 - b. Cardholder IPs
 - c. Transaction Amount
5. There are also two types of lists for the merchant IDs and Cardholder IPs. The type of list you can choose is mutually exclusive.:

a. In List

The merchants and cardholder IPs in this list are mandated to enroll through ADS. Choose this option when you want to configure Adaptive ADS for smaller lists.

b. Not In List

The transactions from the all merchants and cardholder IPs apart from the ones in this list are mandated to enroll through ADS. Choose this option when you want to configure Adaptive ADS for larger lists.

6. To add a merchant ID or cardholder IP to the list, enter the value in the right text box and click **Add**.

NOTE:For cardholder IP, any value from 0 to 255 and * for the last two octets are allowed.

You can select any value in the list and click on **Delete** to remove it from the list.

7. You can also process transaction above a specified amount for any specific currency as an Adaptive ADS transaction.

Click **Submit** after you have entered the appropriate values.

8. The message “*Rules have been added successfully.*” appears.

You can view the rules you have created by selecting the issuer and range as mentioned in steps 1 and 2.

9. The Issuer Configuration Summary report also displays if the range is configured for Adaptive ADS. See the *Arcot TransFort Issuer Software Reports Manual* for more details.

The ACS Callout PAREq Callout is provided to achieve this behavior. When you configure for Adaptive ADS, the PAREq callout is automatically configured for the range. If you want to go beyond these basic capabilities you can configure a different PAREq callout. Adaptive ADS takes precedence over the PAREq callout configuration and they are mutually exclusive. To configure PAREq callout, the basic Adaptive ADS must be cancelled. See “[Cancelling Adaptive ADS](#),” for more information.

NOTE:The callout functionality for this basic Adaptive ADS is shipped with the product.

Figure 8-8 Configuring Adaptive ADS

The screenshot displays a web-based configuration interface for Adaptive ADS. It is divided into three main sections, each with a list of existing values and an 'Add' button for new entries.

- Merchant ID Section:**
 - Header: "Please choose the list to which you want to add/remove Merchant ID's:" with radio buttons for "IN LIST" (selected) and "NOT IN LIST".
 - Existing IDs: A list box containing "18800007013", "tirerack", "4676220000000015", and "5p0ng3b0b5qu8r3-6b1".
 - Action: A "Delete" button next to the list box.
 - Add Field: A text input field followed by an "Add" button.
- Cardholder IP Section:**
 - Header: "Please choose the list to which you want to add/remove Cardholder IP's:" with radio buttons for "IN LIST" (selected) and "NOT IN LIST".
 - Existing IPs: A list box containing "255.2.45.76", "123.45.12.56", and "243.34.12.67".
 - Action: A "Delete" button next to the list box.
 - Add Field: A dotted text input field (e.g., ". . . .") followed by an "Add" button.
- Purchase Amount Section:**
 - Header: "Purchase Amount greater than:".
 - Existing Amount: A list box containing "USD 2000".
 - Action: A "Delete" button next to the list box.
 - Add Field: A dropdown menu (currently showing "--") followed by a text input field and an "Add" button.

Cancelling Adaptive ADS

You can remove the Adaptive ADS configuration from any issuer using the administrative console.

To cancel the Adaptive ADS configuration:

1. Click the **Cancel Adaptive ADS** link in the administrative console.
The Cancel Adaptive ADS page appears.
2. Select the Issuer to be and the appropriate card range or the range group for which you want to remove the Adaptive ADS configuration and press **Submit**.

The message *"Rules cancelled successfully."* appears.

Summary of Cardholder Shopping Experience

The cardholder shopping experience for OptIn and Issuer Activation methods of enrollment is summarized in the table below:

Table 8-3 Cardholder Shopping Experience

Cardholder Action	Password Status	CallOut Status	CAP Page Shown	Cardholder Status	Transaction Status
Chooses to enroll	Available	Not Applicable	Password Page	Activated with password	Authenticated
Chooses to enroll	Not Available	VIA CallOut Configured	“Optin with Issuer Questions page”	Activated with responses to Issuer questions	Authenticated
Chooses to enroll	Not Available	VP CallOut Configured	Password Page	Activated with password	Authenticated
Chooses to enroll later	Not Applicable	Not Applicable	“Continue without Authenticating Transaction Page”	Not Activated	Not Authenticated
Already Active	Available	Not Applicable	“Welcome Page” or “Add secondary Cardholder option”	Active	Authenticated

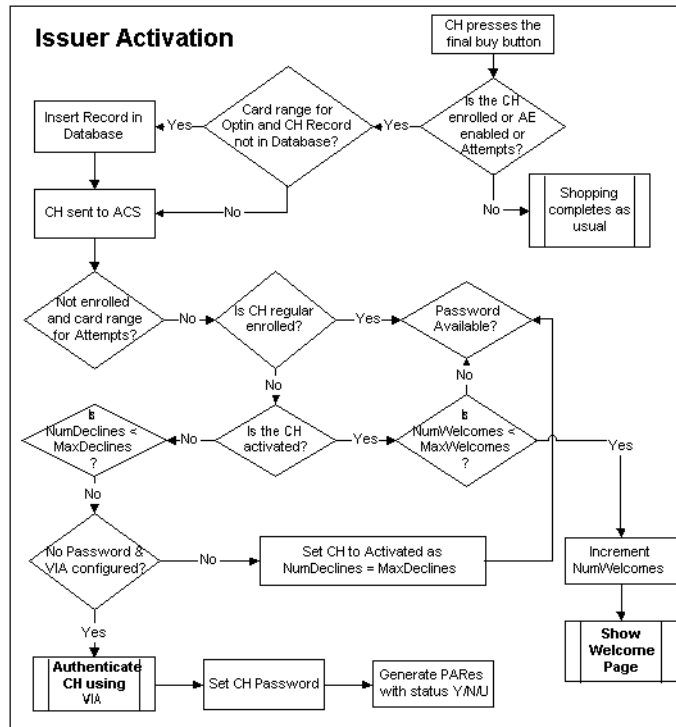
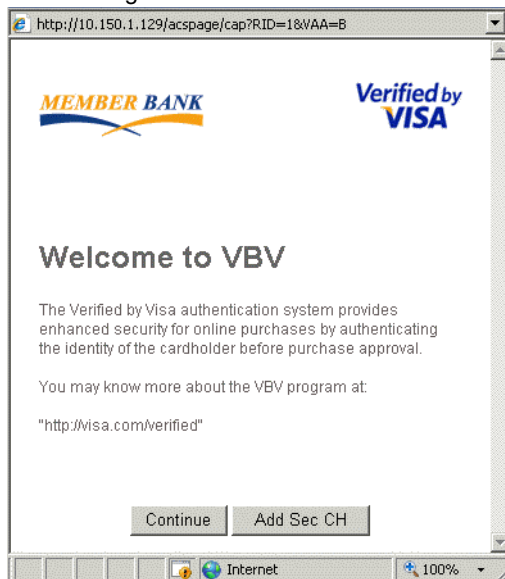
Figure 8-9 Issuer Activation

Figure 8-10 Welcome Page

Purchase Attempts

The cardholder configured for the Attempts feature is introduced to the virtues of the online payer authentication program. The cardholder information is logged in the Issuer Software Database and the purchase continues as a non-authenticated transaction. This information can be used to spotlight active shoppers over the Internet. Such cardholders can be potential candidates for the online payer authentication program. The statistical information can be used as a marketing/sales tool.

When a Issuer wants to configure the ADS to enroll cardholders, the Attempts method can be used first. This can be a first step in the ADS configurations which can be used as a transition to Optin or Issuer Activation methods. The Attempts ADS serves as a proof of attempted authentication for a merchant.

See “[Purchase Attempts](#)” for the process flow. See also the *Arcot TransFort Issuer Software Introduction Manual* for more information about the end user experience.

Requirements of Attempts Feature

1. A Global Administrator creates a card range for the interested Issuers and chooses *Attempts Processing* as the ADS Option.
2. Cardholders are not expected to enroll into the online payer authentication program manually or automatically when this feature is enabled.
3. Cardholders may not be informed about this authentication program
4. To enable Attempts for 3-D Secure 1.0.1 select the `AllowAttemptsfor1.0.1` field in the *ACSCConfig Page* in the administrative console.
5. The ES URL should be changed to the current ES URL in the file `getemail.htm` for cardholder email collection. The file is in the CAP templates folder

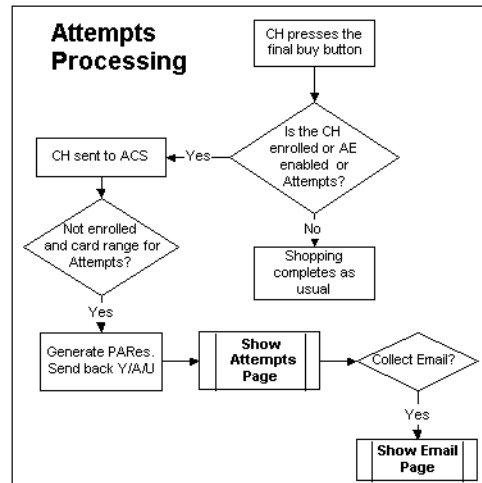
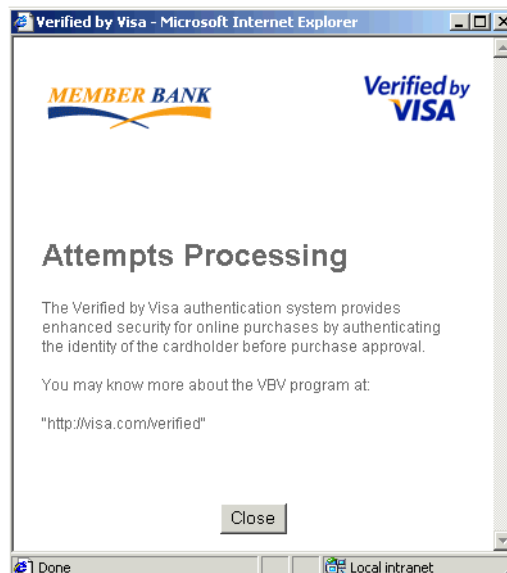
Figure 8-11 Purchase Attempts**Figure 8-12** Attempts Page

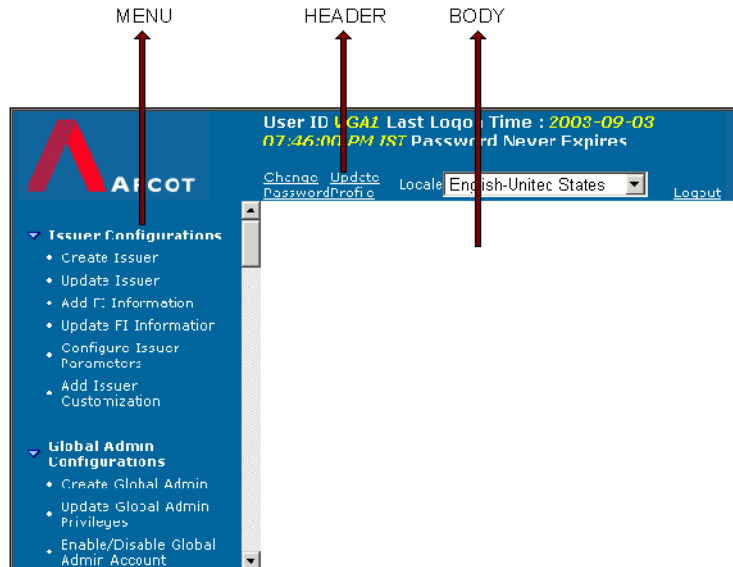
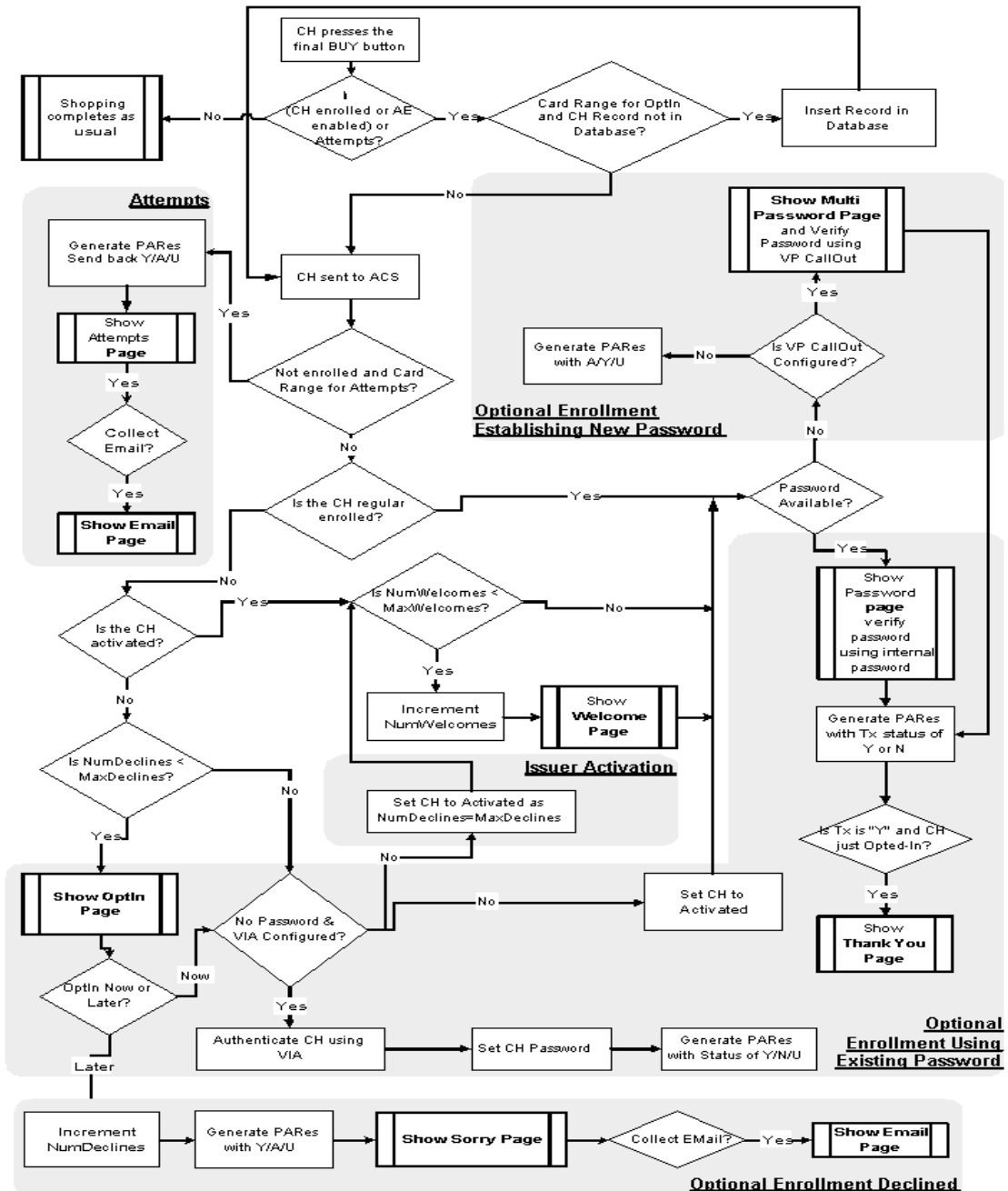
Figure 8-13 EMail Collection Page

Figure 8-14 ADS Flowchart



Issuer Software Configuration and Log Files

This chapter provides descriptions of the following Issuer Software configuration files:

- ACS configuration file (`acs.ini`)
- ACSClient configuration file (`acsclient.ini`)
- CAP configuration file (`cap.ini`)
- Communication parameters configuration file (`comm.ini`)
- ES configuration file (`es.ini`)
- Log file configuration file (`log.ini`)
- ES and Administrative Console Web configuration file (`web.xml`)

This chapter also provides information on the various Issuer Software component log files and guidelines for backing up the configuration files.

NOTE:

The default values displayed in the *.ini tables in this chapter are set during the installation process. See [Appendix C](#) for examples of how the *.ini files look after installation.

ACS Configuration File (acs.ini)

The ACS configuration file, `acs.ini`, contains parameters for configuring the following information applicable to an individual instance of the ACS:

- Communication channels
- Supporting Multiple DS Listeners
- Message handler connection protocols
- Database settings
- Thread settings
- Log file settings
- Crypto device Settings
- AAV Calculation and Instance settings
- Setting Cardholder Personal Message during ADS

The `acs.ini` file is installed to the following default location:

For Windows

```
<$System Root$>:\Program Files\Common Files\  
Arcot Shared\Conf
```

For Unix

```
/opt/arcot/conf
```

The following sections list the applicable parameters for each of the above mentioned categories.

Communication Channels

You can define the communication channels between the ACS and the other components involved in 3-D Secure transaction processing. These channel values are the offsets from the base port values defined in the `comm.ini` file. See “[Communications Configuration File \(comm.ini\)](#)” on page 205 for more information on the `comm.ini` file.

The following table lists the communication channel parameters in the `acs.ini` file and provides descriptions of each:

Table 9-1 Communication Channel parameters in `acs.ini`

Parameter	Default	Description
<code>HTTPDSChannel</code>	21	The offset to the base port used by the ACS DS Message Handler to listen to the HTTP or HTTPS requests coming from the DS. This is the channel used by default.
<code>HTTPDS<N>Channel</code>	No default	The offset to the base port used by the ACS DS Message Handler to listen to the HTTP or HTTPS requests coming from the DS. This is the channel configured to support multiple DS listeners. See “Supporting Multiple DS Listeners,” for more information. Example: <pre>HTTPDS1Channel = 41 HTTPDS2Channel = 42 HTTPDS3Channel = 43 HTTPDS4Channel = 44</pre>
<code>CAPChannel</code>	24	The offset to the base port used by the ACS CAP Message Handler to listen to the SSL or TCP requests coming from the CAP.
<code>AdminChannel</code>	25	The offset to the base port used by the ACS Admin Message Handler to listen to the SSL or TCP requests coming from the CAP.
<code>HTTPAdminChannel</code>	26	The offset to the base port used by the ACS Admin Message Handler to listen to the HTTP or HTTPS requests coming from the ACSClient.

Message Handler Connection Protocols

The ACS spawns three different message handlers:

- **ACS DS Message Handler** - handles messages from the DS regarding 3-D Secure transactions.
- **ACS CAP Message Handler** - handles messages from the CAP like `PARReq`.
- **ACS Admin Message Handler** - handles messages from the `ACSClient` (regarding, for example, graceful shutdown or cache refresh information).

The ACS communicates with the DS using HTTPS connection protocol.

The following table lists the message handler connection protocol parameters in the `acs.ini` file and provides descriptions of each:

Table 9-2 DS and CAP Handler Connection Protocol parameters in `acs.ini`

Parameter	Default	Description
EnableCAPSSL	1	Specifies whether the ACS can use SSL to talk with the CAP.
EnableCAPTCP	0	Specifies whether the ACS can use TCP to talk with the CAP. Caution: TCP communications should only be allowed in situations where communication between the ACS and CAP is routed over secure LANs. Allowing TCP communications between the CAP and the ACS over the Internet opens the entire system to hacker attacks.
EnableAdminSSL	0	Specifies whether the ACS can use SSL to talk to the ACS Admin Message Handler.
EnableAdminHTTPS	1	Specifies whether the ACS can use HTTPS to talk to the ACS Admin Message Handler.

Database Settings

The Database settings in the `acs.ini` file allow you to identify the Issuer Software Database to which the ACS will be connected and a backup database to use for failover. They also let you configure database communications resources available between the ACS and the Issuer Software Database.

As with threads, configuring the maximum and minimum number of communication resources is a trade off between maximizing server efficiency and maintaining system capacity. Specifically, each resource open on a server decreases the server's performance and there is a limit to the number of resources that can be open at any one time before the system's performance falls below acceptable levels. At the same time, limiting the number of resources available limits the number of cardholders that can be accessing the system at any one time.

Maintaining unused communication resources between the ACS and the Issuer Software Database is inefficient. At the same time, opening resources takes three times as many system resources compared to maintaining a previously opened resource. Therefore, opening and closing resources for each user is far less efficient than maintaining a pool of resources available at all times that can be shared by anyone accessing the system.

The trick is to maintain enough resources so that enough resources are maintained to handle average usage levels and allow enough resources to be opened to handle any peak load that the system may encounter.

Furthermore, opening multiple resources at one time is more efficient than opening individual resources one at a time. Therefore, if demand occasionally spikes, it is more efficient to open multiple resources at one time than it is to open resources only as they are requested (in other words, multiple connections will be opened simultaneously to handle the increased demand for resources).

NOTE:

Before you can specify the resources used by the ACS to communicate with the Issuer Software Database, you will need to determine the estimated throughput for the system. For more information on estimating system throughput requirements, see the *Arcot TransFort Issuer Software Introduction Manual*.

The following table lists the database setting parameters in the `acs.ini` file and provides descriptions of each:

Table 9-3 Database Setting parameters in `acs.ini`

Parameter	Default	Description
DBName	XXXXXXXXXX	The name of the ODBC System Data Source Name (DSN) pointing to the primary database hosting the Issuer Software data.
NoBackupDB	0	Indicates that a backup database is configured. Set to 1 if there is no backup database configured.
BackupDBName	No default	The name of the ODBC System DSN pointing to the backup database hosting the Issuer Software data.
UserID	No default	The name of the user ID used by the ACS to access the Issuer Software database.
BackupUserID	No default	The name of the backup user ID used by the ACS to access the Issuer Software Database
MaxDBConns	32	<p>The maximum number of connections that will be created between the ACS and the Issuer Software Database.</p> <p>Note: There is a limit to how many connections an Oracle database will allow and this limit overrides the MaxDBConn parameter. See your Oracle documentation for more information.</p>

Table 9-3 Database Setting parameters in acs.ini

Parameter	Default	Description
MinDBConns	1	The minimum number of connections to initially create between the ACS and the Issuer Software Database.
IncDBConns	2	The number of connections that will be created when a new connection is needed between the ACS and the Issuer Software Database.
MaxDBConnTries	3	The number of times the ACS will attempt to connect to the Issuer Software Database before aborting the connection.
DBConnRetrySleep Time	2000	The number of milliseconds to delay between attempts to connect to the Issuer Software Database.
DBType	oracledb	The type of database management server running the Issuer Software Database. The supported values are: <ul style="list-style-type: none"> • oracledb • db2
DBAutoRevert	0	Specifies whether or not the system will attempt to connect to the primary database after a failover occurs. Set DBAutoRevert=1 if you have a backup Issuer Software Database configured or if you want the ACS to try to connect to the database after a failover occurs.
DBAutoRevertThread Time	3	If DBAutoRevert=1, this parameter specifies the number of seconds between attempts to connect to the primary database.
DBProfiling	0	This parameter specifies if the database messages are being logged. Set to 1 if you want to enable logging of database messages.

Thread Settings

A **thread** is a single sequential flow of control within a program, similar to a process (or running a program) but easier to create and destroy than a process because less resource management is involved. Each thread must have its own resources. In a multi-threaded environment, multiple threads can be spawned and operate simultaneously. This allows the system to share a single environment for all of the threads, reducing the overhead of each individual thread.

There are three factors to consider when determining the maximum and minimum number of threads that will be available for the system:

1. Each thread uses a certain amount of resources and decreases the overall performance of the system.
2. Opening and closing a thread takes up to three times the resources that are required to maintain an open thread.
3. Based on the server's capacity, there is a maximum number of threads that can be opened simultaneously before the server's performance drops below acceptable levels.

The trick is to set the minimum number of threads to handle average system use levels. Set the maximum number of threads at a level high enough to handle any peak load that the system may encounter while maintaining acceptable server performance.

The following table lists the thread setting parameters in the `acs.ini` file and provides descriptions of each:

Table 9-4 Thread Setting parameters in `acs.ini`

Parameter	Default	Description
AdminMaxThreads	16	The maximum number of threads that the ACS Admin Message Handler should contain to connect to the CAP or ACSClient stream pool.
AdminMinThreads	8	The minimum number of threads that the ACS Admin Message Handler should contain to connect to the CAP or ACSClient stream pool.
DSMaxThreads	128	The maximum number of threads that the ACS DS Message Handler will open in order to communicate with the DS or ACSClient.
DSMinThreads	16	The minimum number of threads that the ACS DS Message Handler maintains that are used to communicate with the DS or ACSClient.

Table 9-4 Thread Setting parameters in acs.ini

Parameter	Default	Description
CAPMaxThreads	128	The maximum number of threads that the ACS CAP Message Handler will open in order to communicate with the CAP or ACSClient.
CAPMinThreads	16	The minimum number of threads that the ACS CAP Message Handler maintains that are used to communicate with the CAP or ACSClient.

ACS Log File Settings

The ACS records all system actions that have occurred in a file with a default name of `ArcotACSLog.txt`. The default location of this file is:

For Windows

```
<$System Root$>:\Program Files\Common Files\Arcot
Shared\logs
```

For Unix

```
/opt/arcot/logs
```

You can define a log file name and backup prefix for your ACS log file in `acs.ini`. You can also define the maximum file size of the primary log file. Once the primary log file reaches the maximum size, the file is renamed as follows:

```
Prefix_<LogFileName without extension>_DDMonYY_HH_MM_SS.txt
```

For example:

```
Backup_ArcotACSLog_28Aug02_120258.txt
```

The system will then record new actions in a new primary log file (in other words, in a new instance of `ArcotACSLog.txt`).

The `log.ini` file also contains the same log file setting parameters as those found in `acs.ini`. The settings in `acs.ini` take precedence over the settings in `log.ini`. See [“Log File Configuration File \(log.ini\)” on page 209](#) for more information on `log.ini`.

The following table lists the log file setting parameters in the `acs.ini` file and provides descriptions of each:

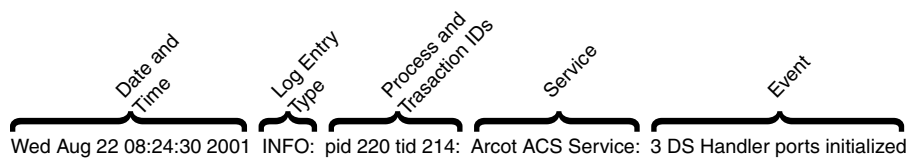
Table 9-5 Log File parameters in `acs.ini`

Parameter	Default	Description
LogfileName	logs/ArcotACSLog.txt	The relative file path to the default directory and the file name of the ACS log file. If this parameter is commented out, ACS will use the <code>LogfileName</code> parameter from <code>log.ini</code> .
RollOverLogPrefix	logs/Backup	The relative file path to the default directory and the prefix to be appended to the log file when the primary log file exceeds the maximum size.
MaxLogfileSize	1048576	The maximum number of bytes the ACS log file can contain..
LogLevel	1	Specifies the granularity of logging. Options are: 1 All messages (INFO, WARN and FATAL) will be logged 2 WARN and FATAL messages will be logged 3 Only FATAL messages will be logged.

ArcotACSLog.txt File Format

ACS records information in the `ArcotACSLog.txt` file as shown in the following figure:

Figure 9-1 ACS Log File Format



The following table describes the components of the message format:

Table 9-6 ArcotACSLog.txt Message Components

Component	Description
Date and Time	The date and time that the event took place.

Table 9-6 ArcotACSLLog.txt Message Components

Component	Description
Log Entry Type	The type of event being logged. Log entry types are as follows: <div> <div>INFO</div> <div>WARN</div> <div>FATAL</div> </div> Normal activities such as port initialization, listeners being started, and so on. Non-fatal system errors, such as failing to connect to the Issuer Software Database, missing parameters in configuration files, and so on. Fatal system errors. Typically, fatal errors occur during startup and are caused by failure to connect to the required service.
Process and Transaction IDs	The process and transaction IDs associated with this event.
Service	The service associated with this event.
Event	The type of event that occurred.

Crypto Device Settings

The ACS uses cryptographic devices to store sensitive keys. Each instance of ACS in your Issuer Software deployment has its own dedicated crypto device.

The following table lists the crypto device parameters in the `acs.ini` file and provides descriptions of each:

Table 9-7 nCipher Information parameters in acs.ini

Parameter	Default	Description
SoftMasterKey	false	<p>Indicates whether or not the Master Key is stored in the crypto device. In a production system, this value is the name of the crypto device in which the Masterkey is stored.</p> <p>This field is case-sensitive. If you comment out this parameter, the ACS assumes a default of false.</p>
nCipherSessions	8	<p>The number of sessions that will be maintained between the ACS and the nCipher hardware accelerator.</p> <p>If you comment out this parameter, the ACS assumes a default of 8.</p>

Table 9-7 nCipher Information parameters in acs.ini

Parameter	Default	Description
PINLOCATION		When set to <code>prompt</code> , the system waits for the Master Key. When the ACS starts the DS and the CAP listeners are not started. The ACS does not attempt to connect to the database and hence the cache is also not loaded into the ACS. Only the Admin listeners in ACS are started. The PIN can be sent to the ACS using the existing command-line tool “ACSCClient.”

AAV Calculation and Instance Settings

Account holder Authentication Value is the cardholder authentication data required by MasterCard for online transactions in which cardholder authentication has been successfully performed. The transportation of AAV in the 3-D Secure PAREs is within the CAVV field. The AAV uses an ACS identifier to identify the instance of the ACS from which the PAREs originated.

Table 9-8 AAV Calculation Settings in acs.ini

Parameter	Default	Description
ACSIdentifierID	0	Identifies the instance of the ACS from which the PAREs originated. This parameter determines the algorithm to calculate the AAV.

NOTE: This is used as a fallback parameter when the range is not configured for AAV algorithm. See [“Adding Financial Institution Information to the Issuer Account,”](#) for more information.

Values for this field are defined based on the algorithm used to create the MAC:

- 0 – 7 Reserved for HMAC
- 8 – 15 Reserved for CVC2
- 16 – 255 – Reserved for future use

Table 9-8 AAV Calculation Settings in acs.ini

Parameter	Default	Description
InstanceId	0	<p>A parameter which can be used to identify any ACS instance. It is recommended that you provide unique values for every instance of ACS.</p> <p>The ACS while sending receipts will look for its unique InstanceId to send receipts generated only by it. The ACS instance is also displayed in the transaction reports, making it easier to trace the ACS to the transaction.</p> <p>IMPORTANT: In a farm of ACS servers, it is strongly recommended that each ACS have a different ID.</p>

Supporting Multiple DS Listeners

The ACS has the ability to support connections from multiple Directory Servers. In version 6.0 and higher, you can also configure separate certificates for each DS connecting to the ACS. It supports a unique ACS-DS listener with its own server certificate, key and client root for every DS connecting to ACS. See [Appendix D, “Certificates Required](#) for the complete list of certificates used by the Issuer Software.

The `acs.ini` will have different channel for each DS that is connecting to it specified in `HTTPDS1Channel`, `HTTPDS2Channel`...`HTTPDS<N>Channel`. Corresponding to every `HTTPDS<N>Channel`, there needs to be:

```
DS<N>SSLClientCACert
DS<N>ServerCertChain
DS<N>SSLServerKey
```

ACS will setup a ‘N’ number of DS listeners with each having its own Client Certificate Root, Server Certificate to present to DS and the corresponding server key. For example,

Table 9-9 Setting Multiple DS Listeners

DS Listener	HTTPS Channel Number	Certificates
Default DS Listener	HTTPDSChannel = 21	DS101SSLClientCACert DS101ServerCertChain DS101SSLServerKey
MasterCard DS Listener	HTTPDS1Channel = 41	DS1SSLClientCACert DS1ServerCertChain DS1SSLServerKey

Table 9-9 Setting Multiple DS Listeners

DS Listener	HTTPS Channel Number	Certificates
Visa DS Listener	HTTPDS2Channel = 42	DS2SSLClientCACert DS2ServerCertChain DS2SSLServerKey

Starting Multiple DS Listeners

When the ACS is starting the DS listeners, it iterates through the list of DS's present in the `acs.ini` file by looking for the format:

```
HTTPDS%dChannel
DS%dSSLClientCACert
DS%dServerCertChain
DS%dSSLServerKey
```

Here, `%d` indicated all the listeners configured from 1 to N. It starts all the listeners configured in the `acs.ini`.

IMPORTANT:

The current DS101* settings will remain unchanged in the `acs.ini` for backward compatibility. If the HTTPDS1* settings is not found, then the ACS will look for the DS101* settings. If both are present, the HTTPDS1* and corresponding DS1* certificate settings will be used.

Message Handler Certificates

The ACS CAP, Admin and DS Message Handlers each use a separate set of certificates for HTTPS/SSL communications. The following table lists the ACS CAP, Admin and DS Message Handler certificate parameters in the `acs.ini` file and provides descriptions of each:

Table 9-10 Message Handler Certificate parameters in `acs.ini`

Parameter	Default	Description
AdminSSLClientCACert	ssl/ClientRootCA.pem	The relative file path and name of the root certificate of the CA that issued certificates to the ACS Admin Message Handler client (ACSClient) for SSL communications to the ACS.
AdminSSLServerCert	ssl/servercert.pem	The relative file path and name of the server certificate that the ACS presents to clients connecting to the ACS Admin Message Handler using SSL.

Table 9-10 Message Handler Certificate parameters in acs.ini

Parameter	Default	Description
AdminSSLServerKey	ssl/serverkey.pem	The relative file path and name of the private key corresponding to the AdminSSLServerCert.
CAPSSLClientCACert	ssl/ClientRootCA.pem	The relative file path and name of the root certificate of the CA that issued certificates to the ACS CAP Message Handler for SSL communications to the ACS.
CAPSSLServerCert	ssl/servercert.pem	The relative file path and name of the server certificate that the ACS presents to clients connecting to the ACS CAP Message Handler for SSL communications to the ACS.
CAPSSLServerKey	ssl/serverkey.pem	The relative file path and name of the private key corresponding to the CAPSSLServerCert.
DS101SSLClientCACert	ssl/ClientRootCA.pem	The relative file path and name of the root certificate of the CA that issued certificates to the DS Message handler for SSL communications for 1.0.1 and later protocol.
DS101SSLServerCertChain	ssl/serverRootCA.pem	The relative file path and name of the server certificate that the ACS presents to clients connecting to the DS Message Handler for SSL communications to the ACS for 1.0.1 and later protocol.
DS101SSLServerKey	ssl/serverkey.pem	The relative file path and name of the private key corresponding to the DS101SSLServerCertChain
DS<N>SSLClientCACert	ssl/ClientRootCA.pem	The relative file path and name of the root certificate of the CA that issued certificates to the DS Message handler for HTTPS communications. This value is present only if you are supporting multiple DS Listeners. See “Supporting Multiple DS Listeners,” for more information.

Table 9-10 Message Handler Certificate parameters in acs.ini

Parameter	Default	Description
DS<N>SSLServerCertChain	ssl/serverRootCA.pem	The relative file path and name of the server certificate that the ACS presents to clients connecting to the DS Message Handler for HTTPS communications to the ACS. This value is present only if you are supporting multiple DS Listeners. See “Supporting Multiple DS Listeners,” for more information.
DS<N>SSLServerKey	ssl/serverkey.pem	The relative file path and name of the private key corresponding to the DS<N>SSLServerCertChain. This value is present only if you are supporting multiple DS Listeners. See “Supporting Multiple DS Listeners,” for more information.

Setting Cardholder Personal Message during ADS

During ADS, the ACS inserts a cardholder enrollment record. You can set a default Personal Message for all the records inserted by ACS in the acs.ini.

Table 9-11 Setting Cardholder Personal Message

Parameter	Default	Description
DefaultPM	Welcome	The default Personal Message you can set for the cardholder when the ACS inserts the cardholder record. This field can be updated when the cardholder chooses to change the Personal Message.

ACSCClient Configuration File (acsclient.ini)

The `acsclient.ini` file serves two purposes: it allows you to configure the ACS DS and Admin Message Handler information to use with the ACSCClient utility, and it allows you to configure CAP connections to one or more ACS instances.

The ACSCClient is a command line utility that is used to refresh certain ACS table cache and to perform a graceful shutdown of ACS. For information on using ACSCClient, see “ACSCClient” in [Chapter 10](#).

The `acsclient.ini` file is installed to the following default location:

For Windows

```
<$System Root$>:\Program Files\Common Files\
Arcot Shared\Conf
```

For Unix

```
/opt/arcot/conf
```

The following table lists the parameters in `acsclient.ini` and provides descriptions of each.

NOTE:

The parameters that contain the word ‘Backup’ (for example, AdminBackupHost) are used for connecting to a backup host when the primary host (for example, AdminHost) is down.

Table 9-12 acsclient.ini parameters

Parameter	Default	Description
AdminHost	localhost	The ACS host name for the CAP or ACSCClient to use to connect to the ACS Admin Message Handler.
AdminBackupHost	localhost	The backup ACS host name for the CAP or ACSCClient to use to connect to the ACS Admin Message Handler.
AdminChannel	26	<p>Deprecated parameter. The ACS channel for the CAP or ACSCClient to use to connect to the ACS Admin Message Handler.</p> <p>If you comment out this parameter, the CAP or ACSCClient assumes a default value of 25.</p> <p>This value is the offset from the base port value set in the <code>comm.ini</code> file. See “Communications Configuration File (comm.ini)” on page 205 for more information.</p>

Table 9-12 acsclient.ini parameters

Parameter	Default	Description
AdminBackupChannel	26	<p>Deprecated parameter. The backup ACS channel for the CAP or ACSCClient to use to connect to the ACS Admin Message Handler.</p> <p>If you comment out this parameter, the CAP or ACSCClient assumes a default value of 25.</p> <p>This value is the offset from the base port value set in the <code>comm.ini</code> file. See “Communications Configuration File (comm.ini)” on page 205 for more information.</p>
AdminPort	9726	The ACS channel for the CAP or ACSCClient to use to connect to the ACS Admin Message Handler.
AdminTransport	HTTPS	The transport protocol the CAP or ACSCClient will use to connect to the ACS Admin Message Handler.
AdminBackupTransport	HTTPS	The backup transport protocol the CAP or ACSCClient will use to connect to the ACS Admin Message Handler.
AdminConnTimeout	0	<p>The number of seconds the CAP or ACSCClient should wait when trying to connect to the ACS Admin Message Handler before the connection times out. 0 indicates no timeout and no attempt is ever made to connect to a backup host.</p> <p>If you comment out this parameter, the ACSCClient assumes a default value of 10.</p>
AdminRespTimeout	0	<p>The number of seconds the CAP or ACSCClient should wait before receiving a response from the ACS Admin Message Handler before the connection times out. 0 indicates no timeout.</p> <p>If you comment out this parameter, the ACSCClient assumes a default value of 10.</p>
AdminServerCACert	ssl/ServerRoot CA.pem	The relative file path and name of the root CA certificate used by the ACSCClient to authenticate the server certificate used by the Admin Message Handler to establish SSL communications with the ACS.

Table 9-12 acsclient.ini parameters

Parameter	Default	Description
AdminClientCert	ssl/ClientCert.pem	The relative file path and name of the client certificate used by an ACS client to establish SSL communications with the ACS.
AdminClientKey	ssl/ClientKey.pem	The relative file path and name of the key associated with the AdminClientCert value.
CAPHostName1	localhost	The primary ACS host name for the CAP or ACSCClient to use to connect to the ACS CAP Message Handler.
CAPHostName2	localhost	The secondary ACS host name for the CAP or ACSCClient to use to connect to the ACS CAP Message Handler.
CAPTransport1	SSL	The primary transport protocol the CAP or ACSCClient should use to connect to the ACS CAP Message Handler.
CAPTransport2	TCP	The secondary transport protocol the CAP or ACSCClient should use to connect to the ACS CAP Message Handler. If you comment out this parameter, the CAP or ACSCClient assumes a default value of SSL.
CAPPortNo1	9724	The primary port the CAP or ACSCClient should use to connect to the ACS CAP Message Handler. If you comment out this parameter, the CAP or ACSCClient assumes a default value of 9724 if CAPTransport1 is set to SSL or 9624 if CAPTransport1 is set to TCP.
CAPPortNo2	9624	The secondary port the CAP or ACSCClient should use to connect to the ACS CAP Message Handler. If you comment out this parameter, the CAP or ACSCClient assumes a default value of 9724 if CAPTransport2 is set to SSL, or 9624 if CAPTransport2 is set to TCP.
ACSConnTimeout1	0	The number of seconds the primary CAP or ACSCClient should wait when trying to connect to the primary ACS CAP Message Handler before the connection times out. 0 indicates no timeout and no attempt is ever made to connect using a secondary source.

Table 9-12 acsclient.ini parameters

Parameter	Default	Description
ACSConnTimeout2	2	The number of seconds the secondary CAP or ACSClient should wait when trying to connect to the secondary ACS CAP Message Handler before the connection times out. 0 indicates no timeout. If you comment out this parameter, the secondary CAP or ACSClient assumes a default value of 0.
ACSRespTimeout1	0	The number of seconds the primary CAP or ACSClient should wait before receiving a response from the primary ACS CAP Message Handler before the connection times out. 0 indicates no timeout.
ACSRespTimeout2	2	The number of seconds the secondary CAP or ACSClient should wait before receiving a response from the secondary ACS CAP Message Handler before the connection times out. 0 indicates no timeout. If you comment out this parameter, the secondary CAP or ACSClient assumes a default value of 0.
CAPMaxConn1	128	The maximum number of connections that the CAP or ACSClient stream pool should contain to connect to the primary ACS CAP Message Handler.
CAPMaxConn2	128	The maximum number of connections that the CAP or ACSClient stream pool should contain to connect to the secondary ACS CAP Message Handler.
CAPMinConn1	16	The minimum number of connections that the CAP or ACSClient stream pool should contain to connect to the primary ACS CAP Message Handler.
CAPMinConn2	16	The minimum number of connections that the CAP or ACSClient stream pool should contain to connect to the secondary ACS CAP Message Handler.
CAPServerCACert1	ssl/ServerRootCA.pem	The relative file path and name of the root CA certificate used by the ACS server for SSL communications.

Table 9-12 acsclient.ini parameters

Parameter	Default	Description
CAPClientKey1	ssl/clientkey.pem	The relative file path and name of the client key used by an ACS client for SSL communications.
CAPClientCert1	ssl/clientcert.pem	The relative file path and name of the client certificate used by an ACS client for SSL communications.

CAP Configuration File (cap.ini)

The CAP acts as a user interface to the ACS. It displays a password pop-up page to cardholders who initiate 3-D Secure purchase transactions at participating merchant sites. The templates for this user interface are installed to the following default location:

For Windows

<\$System Root\$>:\Inetpub\wwwroot\acspage

For Unix

/opt/arcot/CAP/acspage

The `acspage` directory contains localized CAP templates in subdirectories named according to locale (for example, localized French templates are located in the `.\acspage\fr_FR` directory). You can choose to customize these pages for a particular Issuer. See “[Adding Issuer Template Customization](#)” in [Chapter 7](#) for information on customizing these templates.

The `cap.ini` file contains parameters that let you set basic information used by the CAP to display the password user interface pages. The `cap.ini` file is installed to the following default location:

For Windows

<\$System Root\$>:\Program Files\Common Files\
Arcot Shared\Conf

For Unix

/opt/arcot/conf

The following table lists the parameters in the `cap.ini` file and provides descriptions of each:

Table 9-13 cap.ini parameters

Parameter	Default	Description
Debug	0	Indicates whether or not to write additional debug information to the <code>ArcACSlog.txt</code> log file. This parameter is for testing purposes only. Turning on this parameter can affect the performance of your CAP component resulting in lower throughput. After testing, turn this flag back to 0 and restart the web server.

Table 9-13 cap.ini parameters

Parameter	Default	Description
ExecPath	c:\inetpub\ wwwroot\acspage (for windows) or /opt/arcot/C AP/acspage (for unix)	The path to the acspage folder. This directory is the root directory for all of the CAP templates and associated files. If you comment out this parameter, there is no default value.
LogFileName	logs/ArcotCAPLog .txt	The path and filename to the log file for all messages related to CAP. NOTE: If IIS is your web server, ensure that iuser_<machine name> user has write permission on log directory.
DefaultErrorPage	c:\inetpub\ wwwroot\acspage\error.htm (for windows) or /opt/arcot/C AP/acspage/error.htm (for unix)	The default error page displayed for any system error. For example, if the CAP not able to communicate with the ACS, the CAP displays this error page.
PareqLogLevel	0 for no logging 1 for invalid pareq logging 2 for all pareq logging	Indicates whether or not to write PAREq debug information to the ArcACSlog.txt log file. NOTE: Make sure the Debug level in cap.ini is greater than zero.

Communications Configuration File (comm.ini)

The `comm.ini` file allows you to set the base ports for different transport protocol access for the DS, CAP, and Admin Message Handlers to the ACS. It also allows you to define the SSL certificates that enable communication between the ACS and the DS. The `comm.ini` file is installed to the following default location:

For Windows <\$System Root\$>:\Program Files\Common Files\
Arcot Shared\Conf

For Unix /opt/arcot/conf

The ACS SSL certificates should be stored in the following location:

For Windows <\$System Root\$>:\Program Files\Common Files\Arcot Shared\ssl

For Unix /opt/arcot/ssl

For information on installing the SSL certificates, see the *Arcot TransFort Issuer Software Installation Manual*.

The following table lists the `comm.ini` parameters and provides descriptions of each.

NOTE:

The `comm.ini` parameter defaults are set during the installation process. If you comment out any of the `comm.ini` parameters, no other default values are set and the service will not be able to be started. Use caution when changing these parameters.

Table 9-14 comm.ini Parameters

Parameter	Default Value	Description
TCPBasePort	9600	The base port used for both TCP and HTTP communications.
SSLBasePort	9700	The base port used for secure communications including SSL and HTTPS.
SSLCACert	ssl/ServerRootCA.pem	The relative file path and name of the root CA certificate used by the ACS server for SSL communications.
SSLServerKey	ssl/servercertkey.pem	The relative file path and name of the private key corresponding to the SSLServerCert.
SSLServerCert	ssl/servercertkey.pem	The relative file path and name of the server certificate that the ACS presents to clients connecting to the ACS using SSL.

Table 9-14 comm.ini Parameters

Parameter	Default Value	Description
SSLClientCACert	ssl/clientcacert.pem	The relative file path and name of the root certificate of the Certificate Authority which issued certificates to the client (DS).
SSLClientKey	ssl/clientkey.pem	The relative file path and name of the client key used by an ACS client for SSL communications.
SSLClientCert	ssl/clientcert.pem	The relative file path and name of the client certificate used by an ACS client for SSL communications.
sslClientCertChain	ssl/clientchain.pem	The Client Certificate Chain file required when communicating to external SSL servers such as Globeset.
SocketTimeout	0	The number of seconds before a client utility (such as ACSClient) will close a connection to the ACS prior to receiving a response. 0 indicates no timeout.

ES Configuration File (es.ini)

The `es.ini` file allows you to define the connection parameters and the SSL certificates for the ES to use to communicate with the IPGS. The `es.ini` file is installed to the following default location:

For Windows `<$System Root$>:\Program Files\Common Files\
Arcot Shared\Conf`

For Unix `/opt/arcot/conf`

The ES SSL certificates should be stored in the following location:

For Windows `<$System Root$>:\Program Files\Common Files\Arcot Shared\ssl`

For Unix `/opt/arcot/ssl`

For more information on installing the SSL certificates required for IPGS communication, see the *Arcot TransFort Issuer Software Installation Manual*.

For information on globally enabling or disabling IPGS communication for all ES instances in your Issuer Software deployment, see [“Updating the Enrollment Server Configuration”](#).

The following table lists the `es.ini` parameters and provides descriptions of each:

Table 9-15 es.ini Parameters

Parameter	Default	Description
Host	localhost	The IPGS host name or IP address.
Port	1555	The port to use for ES to IPGS connection.
Transport	TCP	The transport protocol used for communications between the ES and the IPGS. This parameter must be set to SSL in order to connect with a live IPGS.
ClientCertPath	None	The file path and name of the client certificate chain.
ClientPrivKeyPath	None	The file path and name of the client private key.
CACertPath	None	The file path and name of the root certificate of the CA used to issue the IPGS certificate.

Table 9-15 es.ini Parameters

Parameter	Default	Description
SocketReceiveTimeoutMS	3000	The number of milliseconds that the ES will maintain an idle connection between the ES and the IPGS. If you comment out this parameter, the ES will wait until the IPGS times out the connection.
JNI Logging Configuration:		The logging configuration for the JNI is found in the section below:
LogFileName		The absolute path and log file name.
BackupLogFile		The backup log file path and name.
MaxLogFileSize		The maximum log file size after which a new log file is started.
LogLevel		Specifies the granularity of logging. The possible options are: <ul style="list-style-type: none"> • 0 - No Logging • 1 - Fatal Messages • 2 - Fatal and Warning • 3 - All messages

Log File Configuration File (log.ini)

The `log.ini` file allows you to configure the primary and backup ACS log files. You can also configure the ACS log files in the `acs.ini` file. The settings in the `acs.ini` file will override the settings in `log.ini`.

For more information on the ACS primary and backup log files, see the [“ACS Log File Settings” on page 190](#).

The `log.ini` file is installed to the following default location:

For Windows

```
<$System Root$>:\Program Files\Common Files\
Arcot Shared\Conf
```

For Unix

```
/opt/arcot/conf
```

The following table lists the `log.ini` parameters and provides descriptions of each:

Table 9-16 log.ini Parameters

Parameter	Default	Description
LogfileName	logs/ArcotLog.txt	The relative file path and name of the ACS log file. If you comment out this parameter, the ACS assumes no other default value.
BackupLogfileName	logs/ ArcotLogBackup.txt	The relative file path and name of the log file to use when the primary log file exceeds the maximum size.
RollOverLogPrefix	logs/Backup	The relative file path and the prefix to be appended to the log file when the primary log file exceeds the maximum size.
MaxLogfileSize	1048576	The maximum number of bytes the ACS log file can contain. If you comment out this parameter, the ACS assumes a default value of 0, indicating no maximum size limit.

Table 9-16 log.ini Parameters

Parameter	Default	Description
LogLevel	1	Specifies the granularity of logging. Options are: 1 All messages (INFO, WARN and FATAL) will be logged 2 WARN and FATAL messages will be logged 3 Only FATAL messages will be logged.

ES and Administrative Console Web Configuration File (web.xml)

The main purpose of the `web.xml` file is to register the Java servlets used by the Enrollment Server and Administrative Console. It also contains configurable elements for the following ES and Administrative Console features:

- Session timeout
- ES log file location
- Back up Issuer Software Database set up
- Crypto Device Settings

The `web.xml` file is installed to the following default location:

For Windows

```
<$System Root$>:\CATALINA_HOME\webapps\web-inf
```

For Unix

```
/Application_Installation_Directory/<WAR-name>/WEB-INF/web.xml
```

Setting Session Timeout

The default session timeout value is ten minutes. This means the Enrollment Server will time out after an inactivity period of ten minutes is reached.

To set the session timeout to another value:

1. Open `web.xml` in a text or XML editor.
2. Locate the following lines of code:

```
<session-config>  
  <session-timeout>10</session-timeout>  
</session-config>
```

3. Change the `<session-timeout>` value to the desired value, as in the following example:

```
<session-config>  
  <session-timeout>30</session-timeout>  
</session-config>
```

4. Save and close the `web.xml` file.

Changing the ES Log File Location

By default, the ES logs the ES log file (event[date].log) to the following directory:

For Windows

```
<$System Root$>:\Program Files\Common Files\Arcot  
Shared\logs
```

For Unix

```
/opt/arcot/logs
```

You can change the directory to which the ES writes the log as desired.

See “[Issuer Software Log Files](#)” on [page 217](#) for more information on the event[date].log file.

To change the ES log file location:

1. Open web.xml in a text or XML editor.
2. Locate the following lines of code:

```
<context-param>  
    <param-name>log.fileName</param-name>  
    <param-value>C:\Program Files\Common Files\Arcot  
Shared\logs</param-value>  
</context-param>
```

3. Change the <param-value> to the desired log location, as in the following example:

```
<context-param>  
    <param-name>log.fileName</param-name>  
    <param-value>C:\temp\logs</param-value>  
</context-param>
```

4. Save and close the web.xml file.

Specifying a Backup Issuer Software Database

To allow the ES and Administrative Console to access a backup Issuer Software Database, you must edit web.xml to include information about the backup database.

This procedure assumes you have already inserted the backup database user name and password into the vpasswd.ini file using DBUtil. See “[Inserting a Backup Issuer Software Database User Name and Password](#)” in [Chapter 10](#) for more information.

For more information on setting up a backup database, see the *Arcot TransFort Issuer Software Installation Manual*.

To specify a backup Issuer Software Database:

1. Open web.xml in a text or XML editor.
2. Locate the following lines of code:

```
<!-- begin of database configuration -->
<context-param>
  <param-name>db.count</param-name>
  <param-value>1</param-value>
</context-param>
<context-param>
  <param-name>db.type</param-name>
  <param-value>oracle</param-value>
</context-param>
<context-param>
  <param-name>db.0.driver</param-name>
  <param-value>oracle.jdbc.driver.OracleDriver
    </param-value>
</context-param>
<context-param>
  <param-name>db.0.url</param-name>
  <param-value>jdbc:oracle:thin:@patna.arcot.com:1521:arc4
    </param-value>
</context-param>
<context-param>
  <param-name>db.0.uid</param-name>
  <param-value>WCdba8CdrNcf4bmmX3a2vg==</param-value>
</context-param>
<context-param>
  <param-name>db.0.maxconn</param-name>
  <param-value>10</param-value>
</context-param>
<!-- end of database configuration -->
```

You will need to edit the existing db.count parameter and add new elements for the backup database.

3. Update the db.count parameter as follows:

```
<!-- begin of database configuration -->
<context-param>
  <param-name>db.count</param-name>
  <param-value>2</param-value>
</context-param>
```

4. Add parameters for the backup database after the `db.0.maxconn` parameter and before the `<!-- end of database configuration -->` comment, as in the following example:

```

<context-param>
  <param-name>db.0.maxconn</param-name>
  <param-value>10</param-value>
</context-param>
<context-param>
  <param-name>db.1.driver</param-name>
  <param-value>oracle.jdbc.driver.OracleDriver
    </param-value>
</context-param>
<context-param>
  <param-name>db.1.url</param-name>
  <param-value>jdbc:oracle:thin:@<host>:<port>:<SID_Name>
    </param-value>
</context-param>
<context-param>
  <param-name>db.1.uid</param-name>
  <param-value><encrypted dbUser></param-value>
</context-param>
<context-param>
  <param-name>db.1.maxconn</param-name>
  <param-value>10</param-value>
</context-param>
<!-- end of database configuration -->

```

5. To obtain the `<encrypted dbUser>` value required for the `db.1.uid` parameter, open the `vpaspwd.ini` file, copy the second to the last value in the list, and paste it into the `<param-value>` tag for `db.1.uid` in `web.xml`.

The second to the last value in the `vpaspwd.ini` file will be the backup database user name *only* if you just ran `DBUtil` to insert the value into `vpaspwd.ini`.

6. Save and close the `web.xml` file.
7. Restart the Enrollment Server.

Crypto Device Settings

The ES Master Key can be stored in a cryptographic device for security reasons. The crypto device parameters to store the key are as follows:

Table 9-17 Crypto Device Settings in ES

Parameter	Description
encryption.key	The base-64 encoded value of the Masterkey label.
encryption.method	<p>The possible methods of encryption:</p> <ul style="list-style-type: none"> • software • hardware <p>If you choose the hardware option, you must also provide the device and <i>numOfSession</i> values.</p>
encryption.device	The possible crypto device which can be used for storing the sensitive keys. See “Determining the crypto device supported” for more information.
encryption.numOfSession	The number of sessions to the crypto device.
encryption.PINLocation	<p>The possible values are:</p> <ul style="list-style-type: none"> • file • prompt <p>If the feature is set to prompt, when the ES starts, it does not attempt to connect to the database and hence the cache is not loaded into the ES. The PIN can be sent to the ES using a new JSP page, <code>ESAdminEnable.jsp</code>.</p>

```
<!-- begin of encryption configuration -->
  <context-param>
    <param-name>encryption.key</param-name>
    <param-value>TWFzdGVyS2V5</param-value>
  </context-param>
  <context-param>
    <!-- encryption method can be software or hardware.
         if it's hardware, pin and numOfSession must have
value
-->
    <param-name>encryption.method</param-name>
    <param-value>hardware</param-value>
  </context-param>
  <context-param>
    <!-- encryption device can be nfast, cca.
```

```
        it's only used with hardware crypto
-->
    <param-name>encryption.device</param-name>
    <param-value>nfast</param-value>
</context-param>
<context-param>
    <param-name>encryption.numOfSession</param-name>
    <param-value>5</param-value>
</context-param>
<context-param>
    <param-name>encryption.PINLOCATION</param-name>
    <param-value>file</param-value>
</context-param>
<!-- end of encryption configuration -->
```

Issuer Software Log Files

The Issuer Software creates different log files to help you monitor system activity and troubleshoot problems. The log files are maintained on the servers on which the applicable Issuer Software component resides (in other words, ES logs are located on the ES machine and ACS logs are located on the ACS machine, if on different machines).

The following log files are available for troubleshooting:

Table 9-18 Issuer Software Log Files

Log File Name	Location	Description
ArcotACSLog.txt	<\$System Root\$>:\Program Files\Common Files \Arcot Shared\logs or /opt/arcot/logs	Records all ACS events in a continuous file. When the maximum file size is reached, the ACS renames the file with a backup prefix and begins a new ACS log. See “ArcotACSLog.txt File Format” on page 191 for more information on this file.
event[date].log	<\$System Root\$>:\Program Files\Common Files\Arcot Shared\logs or /opt/arcot/ES/logs	Records all ES events by day. The ES logs are named event{date}.log, where the date is the current date of the system. Everyday, a new log is created and all events that occur on that day are written to the file.
isapi_redirect.log	<\$System Root\$>:\CATALINA_HOME\logs or /opt/arcot/ES/logs	Records the redirect information from IIS to Tomcat.
catalina_log.date.txt	<\$System Root\$>:\CATALINA_HOME\logs or /opt/arcot/ES/logs	Records the processor logs related to HTTP and AJP connectors.
apache_log.date.txt	<\$System Root\$>:\CATALINA_HOME\logs or /opt/arcot/ES/logs	Logger for Apache-Connector Service

Table 9-18 Issuer Software Log Files

Log File Name	Location	Description
localhost_access_log.date.txt	<\$System Root\$>:\CATALINA_HOME \logs or /opt/arcot/ES/logs	Logger for all requests for this virtual host
localhost_log.date.txt	<\$System Root\$>:\CATALINA_HOME \logs or /opt/arcot/ES/logs	Logger shared by all Contexts related to this virtual host.

Modifying the Enrollment Server Log Settings

You can modify the logging level and directory to which to write the log files for the following Enrollment Server log files:

- catalina_log.txt
- apache_log.txt
- localhost_log.txt

To modify the log file settings:

1. Open the `server.xml` file in a text or XML editor. This file is located in the following directory:

For Windows

<\$System Root\$>:\CATALINA_HOME\conf

For Unix

/opt/arcot/conf

2. Locate the following code section:

```
<Logger className="org.apache.catalina.logger.FileLogger"
    prefix="catalina_log." suffix=".txt"
    timestamp="true"/>
.....
    <Logger className="org.apache.catalina.logger.FileLogger"
        directory="logs" prefix="localhost_log."
suffix=".txt"
        timestamp="true"/>    />
.....
<Logger className="org.apache.catalina.logger.FileLogger"
```

```
prefix="apache_log." suffix=".txt"  
timestamp="true"/>
```

.....

3. To modify the log level, edit the **verbosity** attribute to indicate the desired log level. Levels are as follows:

- 0 - FATAL
- 1 - ERROR
- 2 - WARNING
- 3 - INFORMATION
- 4 - DEBUG

Levels are inclusive; that is, "WARNING" level displays any log message marked as WARNING, ERROR, or FATAL.

In the default `server.xml` code as shown above, the log files do not show the `verbosity` attribute. You may add this attribute to these logs as desired.

4. By default, log files are created in the "logs" directory relative to `$CATALINA_HOME`. If you wish, you can specify a different directory with the "directory" attribute. Specify either a relative (to `$CATALINA_HOME`) or absolute path to the desired directory.
5. When you have finished modifying the code, save and close the `server.xml` file.
6. Re-start the Enrollment Server.

Backing Up Configuration Files

It is good practice to always back up your *.ini configuration files before you make changes to them. Arcot recommends that you store these files in a directory other than

For Windows

```
<$System Root$>:\Program Files\Common Files\  
Arcot Shared\Conf
```

For Unix

```
/opt/arcot/conf
```

in order to ensure that the Issuer Software does not use the backup files instead of the current files. This may happen as the Issuer Software looks for the string “ini” in the final extension of a configuration file and picks up the first file it sees with this string. If your backup configuration files include the string “ini” in the final extension and they reside in the . . \conf directory, the system might use the backup files instead of the real configuration files.

If you want to keep your backup configuration files in the . . \conf directory, ensure that you name your backup files correctly. Examples of incorrectly named backup files and correctly named backup files are as follows:

Incorrect:acs.backup.ini
acs.iniold

Correct: acs.ini.backup
acs_ini.old

Issuer Software Command Line Utilities

This chapter describes the following Issuer Software command line utilities:

- `ACSCClient`
- `DBUtil`
- `PK11 Util`
- `Key Util`

ACSClient

ACSClient allows you to perform the following tasks:

- **Refreshing ACS Cache**
- **Performing a Graceful Shutdown**
- **Key Management**

ACSClient also includes other options to use for testing and diagnostic purposes. These options should only be used under the direction of Arcot Technical Support and thus are not documented in this manual.

Update the `acsclient.ini` file with the applicable parameters for the environment before running ACSClient. ACSClient will only use the primary host parameters in `acsclient.ini`, never the backup parameters. If you want to use ACSClient on a backup ACS, run ACSClient from the backup machine (with the primary host on the backup machine set to localhost). For more information, see the “ACS Client Configuration File(`acsclient.ini`)” section in *TransFort System Operations Manual*.

Refreshing ACS Cache

When the ACS service starts, it creates a cache of Issuer Software Database table data to improve system performance. The ACSClient Refresh Tables command allows you to clear the cache from specified ACS tables after you have made administrative updates to the database without having to shutdown the ACS.

You will want to run this command whenever you update the ACS configuration via the Administrative Console or add a new Issuer account.

To refresh ACS cache:

1. Open a Command prompt.
2. Navigate to the following directory:

- For Windows:

```
<$System Root$>:\Program Files\Arcot Systems\VPAS Server\bin
```

- For Unix:

```
/opt/arcot/bin
```

3. Enter a command using the following syntax:

```
acsclient -r [all bank cap device folder locale useragent  
accept countrycurrency callout]
```

For example:

```
acsclient -r bank
```

ACSCClient refreshes the cache for the specified table(s).

The following table lists the refresh parameters and provides descriptions of each:

Table 6-1 ACSCClient Refresh Parameters

Parameter	Description
all	Refreshes entire ACS cache. Use this parameter when you have made many administrative changes and you are not sure which tables were affected.
bank	Refreshes ACS bank/brand information cache. Use this parameter when you add a new Issuer account or update Issuer information.
cap	Refreshes CAP template cache. Use this parameter when you add a new CAP template directory or change CAP template information.
device	Refreshes ACS Device table cache. Use this parameter when you add a new device to the database.
folder	Refreshes ACS Folder table cache. Use this parameter when you add a new folder for the CAP templates.
locale	Refreshes ACS Locale table cache. Use this parameter if you added a new locale to the database.
useragent	Refreshes ACS HTTP UserAgent table cache. Use this parameter if you add a new User Agent to the database.
accept	Refreshes ACS HTTP Accept table cache. Use this parameter if you add a new accept string to the database.
countrycurrency	Refreshes ACS Country/Currency table cache. Use this parameter if you added a new country or currency code to the database.
callout	Refreshes ACS CallOut table cache. Use this parameter if you added a new ACS callout to the system.

Actions requiring ACS Cache Refresh

The actions following which an ACS cache refresh is required are listed below.

- Any addition, deletion or change to Issuer configuration.
- Any addition, deletion or change to Range configuration.

- Any addition, deletion or change to CallOut configuration.
- Any modifications to ACS configuration parameters.
- Any modifications to the cardholder authentication parameters.
- Any addition or change to support for mobile devices.
- Any addition, deletion or change to CAP templates/folders.

Performing a Graceful Shutdown

The Perform Graceful Shutdown command shuts down the ACS when ACS down-time is known ahead of time. When this command executes, it immediately directs the ACS to stop accepting new connections and new transactions on existing connections. The ACS will wait a specified amount of time for all existing transactions to complete, during which time it will close all idle connections, flush all in-memory cache within ACS to the Issuer Software Database without loss of data, and inform the CAP to failover to another ACS (if a backup ACS is already configured). When the specified time elapses, it will then shutdown the ACS service process.

The specified amount of time to wait is the maximum time the ACS should wait before closing out uncompleted transactions. This ensures that the ACS will shutdown even if one or more connections are stuck or have stalled transactions. Transactions most likely to be affected by a shutdown are Enrollment transactions, as the amount of time a cardholder takes to complete the enrollment process is unpredictable.

If you use the Windows Services utility to shutdown the ACS service instead of ACSCClient, the ACS service will stop immediately regardless of any pending transactions. This will incur a loss of in-process transaction information

To perform a graceful shutdown:

1. Open a Command prompt.
2. Navigate to the following directory:

- For Windows:

```
<$System Root$>:\Program Files\Arcot Systems\VPAS Server\bin
```

- For Unix:

```
/opt/arcot/bin
```

3. Enter the following command:

```
acsclient -gs time
```

where *time* is the number of seconds after which the ACS will shutdown. The minimum value for the *time* parameter is 120 seconds.

For example:

```
acsclient -gs 300
```

This command start the flush of in-memory buffer after 300 seconds, and will shut down acs after flush completes.

Key Management

The Issuer Software ensures complete key protection by using cryptographic hardware like nCipher, IBM crypto devices, etc. The Master Key, used by the Enrollment server and Access Control Server is loaded in a secure cryptographic device like the nCipher box. See “Setting up the Hardware Accelerator in Appendix A of *TransFort System Operations Manual* for more details about the nCipher box.

The TransFort accesses the cryptographic device for all keys. The operator should provide a PIN, called as the operator PIN to access the box. This is not stored anywhere in the Transfort system and is managed as described in the sections below:

Managing the cryptographic device PIN for ACS

The feature can be enabled in ACS by setting a flag in acs.ini file, “PINLOCATION” to “prompt”. See “Crypto Device Settings,” in *TransFort System Operations Manual* for more information. This feature can be disabled by setting this PINLOCATION parameter to any value other than “prompt” or commenting out this parameter altogether.

NOTE:By default this new feature is not enabled.

When the feature is enabled, at start up, the ACS starts the Admin listeners. The DS and CAP listeners are not started. The ACS does not attempt to connect to the database and hence the cache is not loaded into the ACS. The PIN can be sent to the ACS using the existing command-line tool ACSCClient. See “[Transmitting the cryptographic device PIN,](#)” for more details.

The cryptographic device PIN can only be sent from the host machine of the ACS (i.e. localhost or 127.0.0.1), thus removing the security issue of the Key being transmitted over the network.

IMPORTANT: The “NCipher” entry will have to exist in the `vpaspwd.ini` regardless of whether the feature is enabled or not. The value for this entry can be set any junk value (preferred 00000) using the DBUtil tool.

Managing the cryptographic device PIN for ES

The cryptographic device PIN management feature can be enabled in ES by setting a context parameter in `web.xml` file, “`encryption.PINLOCATION`” to “`prompt`”. See “Crypto Device Settings,” in *TransFort System Operations Manual* for more information.

If the feature is enabled, when the ES starts, it does not attempt to connect to the database and hence the cache is not loaded into the ES. The PIN can be sent to the ES using a new JSP page, `ESAdminEnable.jsp`.

To send the cryptographic device PIN to the ES using the jsp, go to the link <http://localhost/vpas/admin/ESAdminEnable.jsp> on the machine running the application server and enter the PIN.

Transmitting the cryptographic device PIN

The “**Key Management**” feature enables the cryptographic device PIN to be “sent” to the ACS and the ES, by the Operator, after the services are started. These services will not be “activated” till the cryptographic device PIN is transmitted.

To transmit the cryptographic device PIN:

1. Open a Command prompt.
2. Navigate to the following directory:

- For Windows:

```
<$System Root$>:\Program Files\Arcot Systems\VPAS Server\bin
```

- For Unix:

```
/opt/arcot/bin
```

3. Enter the following command:

```
acsclient -enable
```

the system prompts the operator for the operator PIN (same as the cryptographic device PIN).

4. Enter the PIN.

The ACS starts successfully if the cryptographic device PIN you have entered is correct.

DBUtil

When the Issuer Software is installed, the installation process creates a `vpaswd.ini` file that stores the Master Key name, Issuer Software Database user name, Issuer Software Database password, and cryptographic device PIN values in encrypted form. `DBUtil` lets you update these values if the need arises. See the *Arcot TransPort Issuer Software Installation Guide* for more information on configuring the primary database.

`DBUtil` allows you to perform the following tasks in the `vpaswd.ini` file:

- Update the Master Key label
- Insert a backup Issuer Software Database user name and password
- Use additional `DBUtil` options

Updating the Master Key Label

The Master Key and Master Key Label are created during the Issuer Software installation process. The Master Key is a triple DES key that is used to encrypt all of the values in the `vpaswd.ini` file. It also encrypts all of the Issuer encryption keys that are stored in the Issuer Software Database. The Master Key is stored on the cryptographic device.

The Master Key Label is stored in the `vpaswd.ini` file in encrypted form. If for some reason you need to change the Master Key Label value in `vpaswd.ini`, run the `DBUtil` as follows.

This procedure assumes you have already created a new Master Key on the cryptographic device. See “[Creating a Master Key](#)” on page 117 for more information.

CAUTION:

This procedure should only be done if the Master Key creation failed during installation. Contact Arcot Technical Support prior to performing this procedure.

To update the Master Key Label:

1. Open a Command prompt.
2. Navigate to the following directory:
 - For Windows:

```
<$System Root$>:\Program Files\Arcot Systems\VPAS Server\bin
```
 - For Unix:

```
/opt/arcot/bin
```

3. Enter the following command:

```
DBUtil -init masterKeyLabel
```

where *masterKeyLabel* is the label for the new Master Key you want to use.

For example:

```
DBUtil -init metrobankMasterKey
```

DBUtil updates the Master Key Name in the *vpaspwd.ini* file.

4. You can also update the Masterkey label stored in the crypto device using the following command:

Usage

```
DBUtil -u <Device Name> <PIN>
```

```
DBUtil -u cca 12345678,
```

where *cca* is the device name. The DBUtil updates the master key label stored in the CCA crypto device.

Inserting a Backup Issuer Software Database User Name and Password

If you are using a backup Issuer Software Database in your deployment, you need to use the DBUtil insert option to add the backup Issuer Software Database user name and password into *vpaspwd.ini*. The DBUtil insert option adds values to the file rather than overwriting (updating) them.

For information on setting up a backup Issuer Software Database, see the *Arcot TransFort Issuer Software Installation Manual*.

For information on configuring the backup Issuer Software Database name and user name for the ACS, for more information see “ACS Configuration File (acs.ini)” in Chapter 9 of *TransFort System Operations Manual*.

For information on configuring the backup Issuer Software Database for the ES, see “Specifying a Backup Issuer Software Database” in Chapter 9 of *TransFort System Operations Manual*.

To insert the Backup Issuer Software Database user name and password into *vpaspwd.ini*:

1. Open a Command prompt.

- Navigate to the following directory:

- For Windows:

```
<$System Root$>:\Program Files\Arcot Systems\VPAS Server\bin
```

- For Unix:

```
/opt/arcot/bin
```

- Enter the following command:

```
DBUtil -pi dbUser dbPassword -h <PIN>
```

where *dbUser* is the backup Issuer Software Database user name defined in the *acs.ini* file and *dbPassword* is the password associated with the backup Issuer Software Database user name.

For example:

```
DBUtil -pi metroBankDb2 metro2 -h 123456
```

DBUtil inserts the backup Issuer Software Database user name and password values in the *vpaspwd.ini* file.

Using Additional DBUtil Options

The following table lists additional options for DBUtil. In this table, *key/value* pair refers to either an Issuer Software Database user name/password pair or an nCipher/nCipher PIN pair. The *key* identifies the *value* being acted upon. For nCipher PIN values, the *key* will always be nCipher.

Table 6-2 Additional DBUtil Options

Option	Description
-pd	Deletes the specified key/value pair from <i>vpaspwd.ini</i> . Syntax: DBUtil -pd <i>key</i> -h <PIN> For example: DBUtil -pd metroBankDb -h 123456

Table 6-2 Additional DBUtil Options

Option	Description
-pi	<p>Inserts an additional key/value pair into <code>vpaspwd.ini</code>.</p> <p>Each key can only have one value. If you have already inserted a key/value pair, you cannot insert another value for the same key. To change a key's value, use <code>-pu</code>.</p> <p>Syntax:</p> <pre>DBUtil -pi key value -h <PIN></pre> <p>For example:</p> <pre>DBUtil -pi nCipher 456789 -h 123456</pre>
-pu	<p>Updates the value for an existing key/value pair in <code>vpaspwd.ini</code>. This feature will most likely be used when you need to update the Issuer Software Database password or cryptographic device PIN value.</p> <p>Syntax:</p> <pre>DBUtil -pu key value -h <PIN></pre> <p>For example:</p> <pre>DBUtil -pu metroBankDb newmetro -h 123456</pre>

PK11 Util

The `PK11 Util` utility allows you to create encryption keys on any of the supported crypto devices. See “Determining the crypto device supported” in *TransFort System Operations Manual* for more information. A `pk11util` command does the following:

1. Identifies the PKCS#11 module and authenticates to it if necessary.
2. Locates a PKCS#11 object on a specified token (e.g. a private key).
3. Performs an action based on that object (e.g. generate, use, destroy).

The usage along with the flags and commands are described in the section below:

Usage

```
pk11util [flags] [index] [command]
```

The following table describes the flag settings for the `pk11util`.

Table 6-3 Flags for PK11 Util

Flag	Description
<code>-module pkcs11_module</code>	Specify the PKCS11 module to use (required). The <code>-module</code> option specifies either the DLL/shared library of the PKCS#11 module directly, or the “name” of the module as specified in the <code>[crypto/pkcs11modules/...]</code> section of <code>pkcs11crypto.ini</code> .
<code>-pin PIN</code>	Specify the PIN to login to the module. If the <code>-pin</code> option is given, the supplied PIN will be used. If neither <code>-pin</code> nor <code>-nopin</code> is specified, <code>pk11util</code> will prompt for a PIN if one is needed. <code>pk11util</code> also supports multiple PINs for k-of-n cardsets.
<code>-nopin</code>	Do not prompt for a PIN, even if one may be required

The following table describes the index options for the `pk11util`.

Table 6-4 Index Options for PK11 Util

Index Options	Description
<code>-cert certfile</code>	Specify an X.509 certificate, use cert public key to find private key

Table 6-4 Index Options for PK11 Util

Index Options	Description
<code>-p7cert p7certfile</code>	Specify an PKCS7 certificate chain, use leaf cert public key to find private key. Example: <pre>pk11util -module nfast -pin 123456 -p7cert "C:\Program Files\Common Files\ArcotShared\NCipher\signcert.p7b" -inform DER</pre>
<code>-inform FMT</code>	Specify input file format (DER or PEM (default)), e.g. for certs. See the example in the previous row.
<code>-slot slotnum</code>	Specify the slot number of the hardware device to use.
<code>-label label</code>	Specify the key label to use.
<code>-app application</code>	Specify an application string for data objects
<code>-bits n</code>	Specify bit length (for generated keys)
<code>-out outfile</code>	Specify output file (e.g. for -genreq)
<code>-outform FMT</code>	Specify output file format (DER or PEM (default))
<code>-inform FMT</code>	Specify input file format (DER or PEM (default)) for certificates
<code>-secure</code>	Use secure or unextractable key flags (e.g. for -importkey)

The following table describes the commands of the pk11util.

Table 6-5 Commands for PK11Util

Command	Description
<code>-query</code>	Query basic information from the module. This option will display information about the specified object, or a general information screen if no particular object has been specified by other options. You can specify a slot number to view all the keys in a particular slot. You can also specify a label with the slot number to view all information about a key in a particular slot.

Table 6-5 Commands for PK11Util

Command	Description
<code>-p7etest</code>	<p>Perform PKCS7 encryption test (encrypt w/public key, decrypt with module private key; requires <code>-cert</code>)</p> <p>Usage:</p> <pre>pk11util -module <module> -pin <pin> -p7etest -cert/-p7cert <Cert> -inform DER [-slot <slot>]</pre> <p>Default inform is PEM.</p>
<code>-destest</code>	<p>Perform DES encryption test with a temporarily created key. (create key, test encryption against test vector; requires <code>-slot</code>).</p> <p>Usage:</p> <pre>pk11util -module <module> -pin <pin> -slot <slot> -destest</pre>
<code>-hmacetest</code>	<p>Perform HMAC-SHA1 test (create key, test MAC against test vector; requires <code>-slot</code>).</p> <p>Usage:</p> <pre>pk11util -module <module> -pin <pin> -slot <slot> -hmacetest</pre> <p>Example:</p> <pre>pk11util -module nfast -pin 123456 -hmacetest -slot 1</pre> <p>Output:</p> <pre>PKCS11 module loaded successfully HMAC-SHA1 digest test PASSED</pre>
<code>-des3cbcmactest</code>	<p>Perform DES3-CBC-MAC test (create key, test MAC against test vector; requires <code>-slot</code>)</p> <p>Usage:</p> <pre>pk11util -module <module> -pin <pin> -slot <slot> -des3cbcmactest</pre> <p>Example:</p> <pre>pk11util -module nfast -pin 123456 -des3cbcmactest -slot 0</pre>

Table 6-5 Commands for PK11Util

Command	Description
<code>-genrsa</code>	<p>Generate an RSA private key in the module (requires <code>-slot</code> and <code>-label</code>). The default keybits for <code>genrsa</code> is 1024.</p> <p>Example:</p> <pre>pk11util -module nfast -pin 123456 -slot 1 -label rsaone_test -genrsa</pre> <p>Output:</p> <pre>PKCS11 module loaded successfully Key generated successfully</pre>
<code>-gendes3</code>	<p>Generate a Triple-DES secret key in the module (requires <code>-slot</code> and <code>-label</code>). The default keybits for <code>gendes3</code> is 168.</p> <p>Example:</p> <pre>pk11util -module nfast -pin 123456 -gendes3 -slot 1 -label test_label3Des</pre>
<code>-gensha1hmac</code>	<p>Generate an NCipher-style HMAC-SHA1 secret key in the module (requires <code>-slot</code> and <code>-label</code>). The default keybits for <code>hmac</code> is 168.</p> <p>Example:</p> <pre>pk11util -module nfast -pin 123456 -gensha1hmac -slot 1 -label testhmac</pre>
<code>-gensec</code>	<p>Generate a 'generic' secret key (e.g. for HMAC) in the module (requires <code>-slot</code> and <code>-label</code>). The default keybits for <code>gensec</code> is 168.</p> <p>Example:</p> <pre>pk11util -module nfast -pin 123456 -gensec -slot 1 -label testsec</pre>
<code>-genreq x500file</code>	<p>Generate a cert request using a key and the name stored in <code>x500file</code> (<code>-out</code> required).</p> <p>Usage:</p> <pre>pk11util -module <module> -pin <pin> -cert\p7cert <cert> -inform <PEM/DER> -outfile <filename> -outform <PEM/DER> -genreq</pre>
<code>-importkey keyfile</code>	Import an RSA key into the module
<code>-importdata datafile</code>	Import file contents into data object in module

Table 6-5 Commands for PK11Util

Command	Description
<code>-hmacsha1 message</code>	<p>Compute HMAC-SHA1 on the given message and key (MC AAV)</p> <p>Usage:</p> <pre>pk11util -module <module> -pin <pin> -slot <slot> -label <label> -hmacsha1 <message></pre> <p>Example:</p> <pre>pk11util -module nfast -pin 123456 -slot 1 -label testhmacsha1 -hmacsha1 "hello World"</pre> <p>Output:</p> <pre>PKCS11 module loaded successfully Base64-encoded MAC: XfzE/hs6BgA4Bh2Vn+MWbrzYrkU=</pre>
<code>-cbcmac message</code>	<p>Compute CBC-MAC on the given message and key</p> <p>Usage:</p> <pre>pk11util -module <module> -pin <pin> -slot <slot> -label <label> -cbcmac <message></pre> <p>Example:</p> <pre>pk11util -module nfast -pin 123456 -slot 1 -label test3Des -hmacsha1 "hello World"</pre> <p>Output:</p> <pre>PKCS11 module loaded successfully Base64-encoded MAC: fJ+hWbWbNJg=MWbrzYrkU=</pre>
<code>-destroy</code>	<p>Remove the named object.</p> <p>For example:</p> <pre>pk11util -module c:\nfast\bin\cknfast.dll -pin 123456 -slot 1 -label testhmac -destroy</pre>

You can use PK11 Util to perform the following tasks:

- Creating Issuer encryption keys

- Creating a Master Key
- Creating Issuer Signing Keys
- Creating HMAC Keys for AAV

Creating Issuer encryption keys

Issuer encryption keys are used to encrypt and decrypt data for the different Issuers you are hosting. Each unique Issuer you are hosting should have its own unique encryption keys (for example, MetroBank and United Bank should have their own unique encryption keys). Issuers who have Issuer accounts in different locales (for example, MetroBank-France and MetroBank-US), can share the same encryption keys.

To generate an Issuer encryption key:

1. Open a Command prompt.
2. Navigate to the following directory:

- For Windows:

```
<$System Root$>:\Program Files\Arcot Systems\VPAS Server\bin
```

- For Unix:

```
/opt/arcot/bin
```

3. Enter the following command:

```
pk11util -module <module_name with path> -slot <slotnum>  
-label <keylabel> -gendes3
```

For example:

For UNIX

```
pk11util -module  
/opt/nfast/toolkits/pkcs11/libcknfast.so -slot 1 -gendes3  
-label metrobankKey
```

For Windows

```
pk11util -module c:\nfast\bin\cknfast.dll -slot 1  
-gendes3 -label metrobankKey
```

pk11util creates the unique key on the cryptographic device.

Use the *label* value (for example, **metrobankKey**) when setting up the Issuer account in the Issuer Software. See “Creating an Issuer Account” in *TransFort System Operations Manual* for more information.

Creating a Master Key

The Master Key and Master Key label are created during the Issuer Software installation process. The Master Key is a triple DES key that is used to encrypt all of the values in the `vpaspwd.ini` file. It also encrypts all of the Issuer encryption keys that are stored in the Issuer Software Database. There is only one Master Key per Issuer Software deployment.

CAUTION:

This procedure should only be done if absolutely necessary. Contact Arcot Technical Support prior to performing this procedure.

To create a new Master Key:

1. Open a Command prompt.
2. Navigate to the following directory:

- For Windows:

```
<$System Root$>:\Program Files\Arcot Systems\VPAS Server\bin
```

- For Unix:

```
/opt/arcot/bin
```

3. Enter the following command:

```
pk11util -module <module_name with path> -slot <slotnum>
-label <keylabel> -gendes3
```

where *keylabel* is the label you want the new Master Key to have

NOTE: Pk11util prompts you to enter the cryptographic PIN.

For example:

For UNIX

```
pk11util -module
/opt/nfast/toolkits/pkcs11/libcknfast.so -slot 1 -gendes3
-label MasterKey
```

For Windows

```
pk11util -module c:\nfast\bin\cknfast.dll -slot 1
-gendes3 -label MasterKey
```

after you provide the PIN, `pk11util` creates the unique key on the cryptographic device.

See “[Updating the Master Key Label](#)” on page 107 for information on how to update the `vpaspwd.ini` file with the new Master Key value.

Creating Issuer Signing Keys

The ACS needs a signing certificate for each Issuer account in order to sign a PAREs. You can use `pk11util` to generate a signing key and certificate request file for an Issuer. `pk11util` generates a private RSA signing key on the cryptographic device and creates a PKCS#10 signing certificate request file in binary or DER format. You can then Base64 encode the certificate request file and submit it to the applicable CA.

To create a private key and generate a certificate request file:

1. Open a Command prompt.
2. Navigate to the following directory:

- For Windows:

```
<$System Root$>:\Program Files\Arcot Systems\VPAS Server\bin
```

- For Unix:

```
/opt/arcot/bin
```

3. Enter the following command:

```
pk11util -module <module_name with path> -slot <slotnum>  
-label <keylabel> -genrsa -genreq <x500name.txt> -out  
<outfile>
```

For example:

```
pk11util -module ibm4758 -slot 0 -label RSAKEY1 -genrsa  
-genreq x500name.txt -out certreq.pem
```

4. The `x500name.txt` contains the DN, e.g, `x500.Arcot.india`. For more information see the *Arcot TransFort Issuer Software Installation Manual* The `pk11 util` generate a key on the cryptographic device and creates a certificate request file.

To get the corresponding certificate, send the Certificate Request (`certreq.pem`) to the respective CA. The CA will return your certificate and chain of certificates.

5. When you receive the requested certificate from the CA, combine the signing certificate, the CA root certificate, and any intermediate certificates into a PKSC#7 certificate chain (for example, `ACSCert.p7b`). Then update the Issuer account with the certificate information. See “Updating the Financial Institution Information” of *TransFort System Operations Manual* for more information.

Creating HMAC Keys for AAV

The Accountholder Authentication Value (AAV) appears on a PAREs confirming that cardholder authentication has been successfully performed. The key for AAV calculation is a Keyed-Hash Message Authentication (HMAC) Code. You can use the `pk11util` command line utility to generate the HMAC key required to calculate the AAV.

To create a HMAC key:

1. Open a Command prompt.
2. Navigate to the following directory:

- For Windows:

```
<$System Root$>:\Program Files\Arcot Systems\VPAS Server\bin
```

- For Unix:

```
/opt/arcot/bin
```

3. Enter the following command:

```
pk11util -module <module_name with path> -genshahmac -slot  
<slotnum> -label <keylabel>
```

For example:

```
pk11util -module nfast -pin 123456 -genshahmac -slot 1  
-label testhmacsha1
```

This command creates a HMAC key in the specified slot.

4. You must provide this key label in the **SecureCode Key Alias** field in the Add FI Info page.

See “Obtaining the HMAC key for AAV Calculations,” in *TransFort System Operations Manual* for more information.

Key Util

The Key Util allows you to create the CVV keys on the crypto device you have setup. The following sections explain the Key Util utility with the usage and option settings.

Usage

```
keyutil [options] [commands]
```

The following tables describe the options and the commands for the utility:

Table 6-6 Options for Key Util

Options	Description
-module module	Specify the cryptographic module to use.
-o options	Specify the module options.
-label label	Specify the key label.
-bits bits	Specify bit length (for generated keys).

Table 6-7 Commands for Key Util

Commands	Description
-genkey type	Generate a key of the specified type (e.g. 3DES, CVV). Usage: <pre>keyutil -module ibm4758 -label CVVKEYA,CVVKEYB -genkey CVV</pre>
NOTE: The key label can be of any length upto a maximum of 16 alphanumeric characters.	
-cvv PAN EXP SVCC	Compute a VISA CVV on the specified data.
-hmacsha1 message	Compute HMAC-SHA1 on the specified message.

See “Creating CVV keys for CAVV,” in *TransFort System Operations Manual* for an example on how to use the Key Util to generate the CVV keys.

Setting Up Third-Party Hardware Components

This appendix contains set up information for the following Third-party hardware components used by the Issuer Software:

- [Setting Up the Host Security Module*](#)
- [Setting Up the Hardware Accelerator](#)
- [Setting Up IBM Cryptocard 4758](#)

**.Applicable only for Visa configurations.*

Setting Up the Host Security Module

In an Issuer Software deployment, the Host Security Module (HSM) is used to calculate Card Verification Values (CVVs)* and to enable chip card support. The Issuer Software currently works with the Thales e-Security (formerly known as Zaxus) RG7000 HSM.

This appendix assumes you have already completed the HSM installation as outlined in the Thales e-Security *Host Security Module RG7000 Operations and Installation Manual*.

This appendix provides brief outlines of the following tasks required to set up the HSM to work with the Issuer Software:

- Configure the HSM
- Set up key management
- Enable CVV calculations
- Enable chip card support

Please refer to the Thales e-Security *Host Security Module RG7000 Operations and Installation Manual* for detailed information on completing each task, except where otherwise indicated.

Configuring the HSM

Complete the following tasks to configure the HSM:

1. Validate the Visa ARQC (Authorization Request Cryptogram) by running the **KQ** host command.

This requires the firmware version to be 0007-E001. To check the HSM version, open the box and locate chips U24 and U25. If either chip label indicates a different version, contact Thales e-Security to request the correct chips.

See the Thales e-Security *Host Security Module RG7000 Programmer's Manual* for detailed information on the **KQ** command.

2. Connect the power to the HSM and perform a cold start. Connect the battery in order to maintain the LMK and software configuration parameters during a power failure.
3. Configure the Console Port Default Settings as described in the Thales e-Security *Host Security Module RG7000 Operations and Installation Manual*.

**.Applicable only for Visa configurations.*

4. Connect to the HSM using a dumb terminal or a terminal running Microsoft Windows NT's HyperTerminal utility.

If you are connecting to a Production system, use a dumb terminal to ensure no data is stored.

5. Configure the console as desired using the **CC** command.
6. Configure the security commands using the **CS** command. Accept the default values, with the following exceptions:

Echo Password and Secret Values to Console:	Off
Availability of clear PIN facility:	No
Availability of ZMK translate command:	Yes
Availability of ANSI X9.17 methods for importing keys:	Yes
Availability of ANSI X9.17 methods for exporting keys:	Yes
Zone Master Key Length:	Double

7. Configure the ethernet connection to the LAN as needed, and do the following:
 - a. Use the 15-way D-Type 10-Base5 connector.
 - b. Obtain a static IP address and connection port.
 - c. Configure the TCP/IP connection using the **CH** command. Accept the defaults, with the following exceptions:

Message Header length:	16
Protocol:	Ethernet
Character format:	ASCII
UDP:	No
TCP:	Yes
Number of Connections:	8

Setting Up Key Management

Complete the following tasks to set up key management:

1. Generate the LMK components using the **GK** command.
2. Load the LMK components using the **LK** command.
3. Install or generate the ZMK (referred to by Visa as ZCMK) according to Issuer guidelines.

The following process needs to be followed whenever the ZMK components are changed or if Issuers choose to generate their own ZMK:

- a. Three security officers representing the Issuer or Visa come to the HSM location.
- b. The HSM host operator inputs the appropriate password into the HSM to enter the authorized state.
- c. The HSM host operator enters the **FK** command.
- d. Each security officer inputs one ZMK component.

The LMK encrypts each ZMK component.

Enabling CVV Calculations

Complete the following tasks to set up CVV calculation support:

1. Obtain a CVK pair by doing one of the following:
 - Generate a new CVK pair using the **KA** command.
If the new CVK pair needs to be shared among multiple sites, export the pair using the **KE** command.
 - Import an existing CVK pair using the **IK** command.
2. Add the CVK pair values to the Issuer Software Database. See [“Adding Financial Institution Information to the Issuer Account”](#) for more information.

Enabling Chip Card Support

You can enable chip card support in test and production environments.

To enable chip card support in a test environment:

1. Calculate the encrypted MDK value using the **FK** command. Use the following parameters:

Enter key length:	2
Enter key type:	109
Enter key scheme:	U
Enter component type:	X
Enter number of components:	1
2. Add the encrypted MDK value to the Issuer Software Database. See [“Adding Financial Institution Information to the Issuer Account”](#) for more information.

To enable chip card support in a production environment:**NOTE:**

This procedure assumes the MDK was created on another HSM and needs to be imported under the control of the Visa ZCMK.

1. Obtain the ZMK value.
2. Import the MDK using the **IK** command. Use the following parameters:

Enter key type:	109
Enter key scheme:	U
3. Add the encrypted MDK value to the production Issuer Software Database. See [“Adding Financial Institution Information to the Issuer Account”](#) for more information.

Setting Up the Hardware Accelerator

The Issuer Software uses the nCipher payShield hardware accelerator to store the Master Key, Issuer Encryption Keys, and Issuer Signing Keys. Each machine running either the ACS or ES has at least one nCipher box attached to it. The Issuer Software requires you to set up a security world to enable key management among the hardware accelerators in your deployment. See “[Key Management](#)” on page 225 for more information.

This appendix assumes you have already completed the nCipher installation as outlined in the applicable nCipher *Hardware Installation Guide*.

This appendix provides brief outlines of the following tasks:

- [Setting up a Security World](#)
- [Creating the Master Key](#)
- [Creating the Issuer Encryption Key](#)
- [Creating CVV keys for CAVV](#)
- [Creating Signing Keys](#)
- [Adding an Accelerator to the Security World](#)
- [Adding New Issuer Keys to the Security World](#)

Please refer to the nCipher *Key-Loading Solution Guide* for detailed information on completing each task, except where otherwise indicated.

Setting up a Security World

Your Issuer Software deployment may include multiple nCipher boxes. Set up the security world on one nCipher box prior to installing the Issuer Software. After you install the Issuer Software and generate the applicable keys on the first nCipher box, you can add other nCipher boxes to the security world. See “[Adding an Accelerator to the Security World](#)” later in this chapter for details.

To set up a security world:

1. Start the accelerator in the pre-initialization state.
2. On the applicable machine, open a Command prompt and navigate to the following directory:

```
<$System Root$>:\nfast\bin
```

3. Create the security world using the **sw-init** command.
4. Answer the prompts as applicable to your installation.

IMPORTANT: Issuer Software and the other command line tools mandates the hardware device has to be accessible with the use of just one operator card. The operator card contains the key to access the cryptographic device & the corresponding PIN. The m*n configuration cannot be used as the card has to be present in the slot during production time and more than one card cannot be inserted into the slot at the same time.

5. When you have completed the initialization, restart the accelerator in the operational state.
6. Create the operator card by doing the following:
 - a. Insert the operator smart card in the reader.
 - b. Enter the following command:

```
ckinittoken userPassword label [-persistent]
```

where *userPassword* is the operator card pass phrase (also known as the nCipher PIN), *label* is the name of the operator card, and *-persistent* makes the card token persistent.

For example:

```
ckinittoken 123456 metroBankOpCard -persistent
```

For more information on the `ckinittoken` command, see the nCipher *PKCS #11 Library User's Guide*.

After you set up the security world on one nCipher box, you can create the required keys on that box. The following sections describe the procedure to create keys that the Issuer Software stores on the nCipher box and provides information on how to generate each key.

Creating the Master Key

The Master Key is a DES key that is used to encrypt values such as the Issuer Encryption Key Labels, the Issuer Software Database User name and password, and so on. There is only one Master Key per Issuer Software deployment.

The Master Key is automatically generated during Issuer Software installation. If necessary, you can create a new Master Key using the `pk11` utility. See [“Creating a Master Key”](#) in [Chapter 10](#) for more information.

Usage `pk11util -module c:\nfast\bin\cknfast.dll -pin 12345678 -slot 0
-label MasterKey -gendes3`

cca is the device which holds the MasterKey and 12345678 is the pin of the device

You have run the following commands to load the master key in the `vpaspwd.ini` file. The “**DBUtil**,” command line utility is used to do the same.

Usage

```
DBUtil -init MasterKey
DBUtil -i nfast <pin>
DBUtil -pi <username> <password> -h <pin> -d nfast
```

Creating the Issuer Encryption Key

The Issuer Encryption keys are triple DES keys used to encrypt and decrypt data for the different Issuers you are hosting. You generate the Issuer Encryption Keys using the `pk11` utility. See “**Creating Issuer encryption keys**” in **Chapter 10** for more information.

1. Generate the Issuer Encryption key using the `pk11` utility:

Usage `pk11util -module c:\nfast\bin\cknfast.dll -pin <pin> -slot 0
-label BankKey -gendes3`

Here BankKey is the Bank Key

2. In the **Update ACSConfig** page in the administrative console, set the device name. Choose **HSM1Device** to nfast.
3. In the **Add FI Information** page and set the Bank Key Module. Choose the **Bank Key Module** to be nCipher-nShield.
4. Provide the bank key label in the **Encryption Key** in the Create Issuer page. This label is encrypted with the masterkey and stored in the database.

Creating CVV keys for CAVV

The Cardholder Verification Value (CVV) Keys are single-length DES key pairs used to calculate CAVVs. The CAVV appears on a PAREs to confirm cardholder authentication was performed.

1. Generate the CVV key pair using the **KeyUtil** command line utility.

Usage

```
keyutil -module c:\nfast\bin\cknfast.dll -label CVVKEYA,CVVKEYB
-genkey CVV
```

2. In the **Update ACSConfig** page in the administrative console, set the device name.
Choose HSM1Device to nfast.
3. In the **Add FI Information** page and the **Create Issuer** page, set the Authentication Key Module.
Choose the **Authentication Key Module** to be nCipher-payshield.
4. You can provide the CVV keys at the issuer level or at the range level.
 - a. To provide the keys at the Issuer level, enter the keys in the **Create Issuer** page.
 - b. To provide the CVV keys at the range level, enter the keys in the **Add FI Information** page.

Creating Signing Keys

The RSA signing keys are used to sign Payer Authentication Responses (PAREs). You can generate new Issuer Signing Keys using the `pk11util` utility. See “[PK11 Util](#)” in [Chapter 10](#) for more information.

To generate and import the signing keys in nCipher:

1. Generate an RSA key

```
pk11util -module c:\nfast\bin\cknfast.dll -slot 0 -label
RSAKEY1 -genrsa -genreq x500name.txt -out certreq.pem
```

The x500name.txt contains the DN, e.g, x500.Arcot.india. To get the corresponding certificate, send the Certificate Request (certreq.pem) to the respective CA. The CA will return your certificate and chain of certificates.

For more information see the *Arcot TransFort Issuer Software Installation Manual*

2. In the **Add FI Information** page, set the Signing Key Module.
Choose the **Signing Key Module** to be nCipher-nShield.
3. Provide the full path to the certificate files in the **Add FI Information** page to load the certificates into the database.

Adding an Accelerator to the Security World

When you have generated your Issuer Software Keys on one nCipher box, you can make those keys available to all nCipher boxes in your deployment by adding each box to the security world.

To add an accelerator to the security world:

1. Start the accelerator in the pre-initialization state.
2. If the additional nCipher box is connected to a different computer than the first nCipher box, copy the `<$System Root$>:\nfast\kmdata` directory from the first computer to the same directory on the applicable computer.

The `.. \kmdata` directory contains the security world key management data.

3. On the applicable computer, open a Command prompt and navigate to the following directory:

```
<$System Root$>:\nfast\bin
```

4. Enter the `sw-rest` command.
5. Answer the prompts as applicable to your installation.
6. When you have completed the initialization of the new accelerator, restart the accelerator in the operational state.

Adding New Issuer Keys to the Security World

After you have set up your entire security world and your Issuer Software hosting site needs to support a new Issuer account, you can easily make the Issuer Encryption Keys and Signing Keys available to all nCipher boxes in your deployment.

To add new Issuer Keys to the security world:

1. Generate the new Issuer Keys as described in the previous sections on one nCipher box.
2. Copy the `<$System Root$>:\nfast\kmdata` directory from the first computer to the same directory on all applicable computers.

Setting Up IBM Cryptocard 4758

The IBM 4758 PCI Cryptographic Coprocessor adds a high-security environment to your server systems for DES, RSA, and DSA cryptographic functions and sensitive custom applications.

TransFort Issuer Software requires a minimum of two IBM 4758 (CCA version 02.41) modules, one configured for PKCS#11 operation and one configured for CCA. Both modules will be performing key management functions. The IBM Common Cryptographic Architecture (CCA) interface provides many functions of special interest in the finance industry (like CAVV calculation) while PKCS#11 interface is used for encryption, decryption and signing.

The following section describes how to generate:

- Encryption keys
- RSA signing keys
- CVV keys for financial calculations

NOTE: We are assuming that the IBM 4758 card and the appropriate drivers are loaded. The setup of the card is completed and the card is ready to generate and store keys.

Creating the configuration files

You have to create configuration files `ccacrypto.ini` and `pkcs11crypto.ini` and modify the `acs.ini`.

1. Create the **ccacrypto.ini** in the `/opt/arcot/conf` directory and add the following lines:

```
[crypto/modules/cca]
sharedlibrary=/opt/arcot/lib/libccacrypto.so
[crypto/modules/ibm4758]
sharedlibrary=/opt/arcot/lib/libccacrypto.so
```

2. Create the **pkcs11crypto.ini** in the `/opt/arcot/conf` directory and add the following lines:

```
[crypto/pkcs11modules/cca]
sharedlibrary=/usr/lib/pkcs11/PKCS11_API.so
[crypto/pkcs11modules/ibm4758]
sharedlibrary=/opt/arcot/lib/libccacrypto.so
```

3. Modify the `acs.ini` located in the `/opt/arcot/conf` directory:

Locate the following lines and modify the settings as shown below:

```
SoftwareMasterKey=cca //means the MasterKey is there in cca
PINLocation=cca
```

4. Now add the following lines in `acs.ini`

```
[arcot/vpas/acs/cca]
PinLocation=cca
```

Creating the Master Key

The Master Key is a DES key that is used to encrypt values such as the Issuer Encryption Key Labels, the Issuer Software Database User name and password, and so on. There is only one Master Key per Issuer Software deployment.

The Master Key is automatically generated during Issuer Software installation. If necessary, you can create a new Master Key using the `pk11` utility. See [“Creating a Master Key”](#) in [Chapter 10](#) for more information.

Usage `pk11util -module cca -pin 12345678 -slot 0 -label MasterKey -gendes3`

`cca` is the device which holds the MasterKey and `12345678` is the pin of the device

You have run the following commands to load the master key in the `vpaspwd.ini` file. The [“DBUtil,”](#) command line utility is used to do the same.

Usage `DBUtil -init MasterKey`
`DBUtil -i cca <pin>`
`DBUtil -i ibm4758 <pin>`
`DBUtil -pi <username> <password> -h <pin> -d cca`

Creating the Issuer Encryption Key

The Issuer Encryption keys are triple DES keys used to encrypt and decrypt data for the different Issuers you are hosting. You generate the Issuer Encryption Keys using the `pk11` utility. See [“Creating Issuer encryption keys”](#) in [Chapter 10](#) for more information.

1. Generate the Issuer Encryption key using the `pk11` utility:

Usage `pk11util -module cca -pin <pin> -slot 0 -label BankKey -gendes3`

Here BankKey is the Bank Key

2. In the **Update ACSConfig** page in the administrative console, set the device name.
Choose HSM1DeviceName to cca.
3. In the **Add FI Information** page and set the Bank Key Module.
Choose the **Bank Key Module** to be **IBM Crypto**.
4. Provide the bank key label you use in the **Encryption Key** field in the Create Issuer page. The value is encrypted with the masterkey and stored in the database.

Creating CVV keys for CAVV

The Cardholder Verification Value (CVV) Keys are single-length DES key pairs used to calculate CAVVs. The CAVV appears on a PAREs to confirm cardholder authentication was performed.

1. Generate the CVV key pair using the **KeyUtil** command line utility.

Usage

```
keyutil -module ibm4758 -label CVVKEYA,CVVKEYB -genkey CVV
```

2. In the **Update ACSConfig** page in the administrative console, set the device name.
Choose HSM1DeviceName to cca.
3. In the **Add FI Information** page and the **Create Issuer** page, set the Authentication Key Module.
Choose the **Authentication Key Module** to be **IBM Crypto**.
4. You can provide the CVV keys at the issuer level or at the range level.
 - a. To provide the keys at the Issuer level, enter the keys in the **Create Issuer** page.
 - b. To provide the CVV keys at the range level, enter the keys in the **Add FI Information** page.

Creating Signing Keys

The RSA signing keys are used to sign Payer Authentication Responses (PAREs). You can generate new Issuer Signing Keys using the **pk11util** utility. See [“PK11 Util”](#) in [Chapter 10](#) for more information.

To generate and import the signing keys in the IBM card:

1. Generate an RSA key

```
pk11util -module ibm4758 -slot 0 -label RSAKEY1 -genrsa  
-genreq x500name.txt -out certreq.pem
```

The x500name.txt contains the DN, e.g. x500.Arcot.india. To get the corresponding certificate, send the Certificate Request (certreq.pem) to the respective CA. The CA will return your certificate and chain of certificates.

For more information see the *Arcot TransFort Issuer Software Installation Manual*

2. In the **Add FI Information** page, set the Signing Key Module.

Choose the **Signing Key Module** to be **IBM Crypto**.

3. Provide the full path to the certificate files in the **Add FI Information** page to load the certificates into the database.

Error Codes

This appendix contains the following tables that list the error codes that are found in the Access Control Server (ACS) component of the Issuer Software:

- Transaction Detail Status Codes
- Processing Errors

If you experience problems with the Arcot Issuer Software, you should contact Arcot Customer Support.

Arcot Customer Support: 1.408.969.6250

Transaction Details Status Codes

Table B-1 Transaction Details Status Codes

Status Codes	Description
000	Core Payer Authentication successful.
001	Core Payer Authentication cancelled on Password page.
002	Core Payer Authentication failed.
003	Core Payer Authentication cancelled on Hints page.
011	Core Payer Authentication failed. ACS database error.
020	Core Payer Authentication failed. ACS Web interface error.
030	Core Payer Authentication failed. Directory Server system error.
031	Core Payer Authentication failed. Directory Server database error.
040	Core Payer Authentication failed. MPS system error.
050	Core Payer Authentication failed. Verification Server system error.
100	Chip Card Authentication successful.
101	Chip Card Authentication failed. No ARQC generated.
102	Chip Card Authentication failed. ARQC could not be validated.
103	Chip Card Authentication failed. No eAccess application found on card.
104	Chip Card Authentication failed. Installed software faulty.
110	Chip Card Authentication failed. ACS system error.
120	Chip Card Authentication failed. ACS Web interface error.
130	Chip Card Authentication failed. Directory Server system error.
140	Chip Card Authentication failed. MPS system error.
150	Chip Card Authentication failed. Verification Server system error.
160	Chip Card Authentication failed. Secret password not valid.
170	Chip Card Authentication failed. General failure caused by secret password.
199	Chip Card Authentication failed. General failure.
200	Token Card Authentication successful.
201	Token Card Authentication cancelled on the Password page.

Table B-1 Transaction Details Status Codes

Status Codes	Description
202	Token Card Authentication failed. Token PIN not valid.
210	Token Card Authentication failed. ACS system error.
213	Token Card Authentication failed. Authentication Server not available.
214	Token Card Authentication failed. Challenge not returned by the Authentication Server.
220	Token Card Authentication failed. ACS Web interface error.
230	Token Card Authentication failed. Directory Server system error.
240	Token Card Authentication failed. MPS system error.
250	Token Card Authentication failed. Verification Server system error.
800	ArcotID Authentication successful.
802	ArcotID Authentication failed. ArcotID PIN not valid.
810	ArcotID Authentication failed. ACS system error.
813	ArcotID Authentication failed. Arcot Authentication Server is not available.
814	ArcotID Authentication failed. Challenge not returned by the Arcot Authentication Server.
820	ArcotID Authentication failed. ACS Web interface error.
830	ArcotID Authentication failed. Directory Server system error.
840	ArcotID Authentication failed. MPS system error.
850	ArcotID Authentication failed. Verification Server system error.

Processing Errors

Table B-2 Processing Errors

Error Code	Description
1000	ACS error. ACS was unable to verify enrollment.
1001	ACS error. Password screen could not be constructed.
1002	ACS error. An error occurred while verifying the cardholder's password.
1003	ACS error. Cannot retrieve hint question.
1004	ACS error. Cannot verify answer for the hint question.
1005	ACS error. PAREs generation error.
1006	ACS error. PAREs signing error.
1007	ACS error. Receipt generation error.
1008	ACS error. Receipt saving error.
1009	ACS error. Cannot verify card range.
1010	ACS error. Invalid request message.
1011	ACS error. No ACS database connection available.
1012	ACS error. Daughter window session time-out.
1013	ACS error. Receipt queue is full.
1014	ACS error. Credit card has expired.
1015	ACS error. Arcot Authentication Server is not available.
1016	ACS error. Cannot verify secret associated with the Chip Card.
1017	ACS error. Host security module box is down.
1018	ACS error. The HSM verify ARQC failed.
1019	ACS error. The ACS Client timed out.
1020	ACS error. Invalid Currency Code.
1021	ACS error. Invalid Country Code.
1022	ACS error. Amount and Purchase Amount mismatch.
1023	ACS error. Invalid end recurring payment date format.
1024	ACS error. Invalid card expiration date format.
1025	ACS error. Invalid end recurring payment date.

Table B-2 Processing Errors

Error Code	Description
1026	ACS error. Invalid VEReq extension critical value.
1027	ACS error. Cannot handle VEReq extension element.
1028	ACS error. Invalid PAREq extension critical value.
1029	ACS error. Cannot handle PAREq extension element.
1030	ACS error. ACS operation failed.
1031	ACS error. ACS transport exception thrown.
1032	ACS error. ACS Client read error.
1033	ACS error. ACS shutdown initiated from Admin.
1034	ACS error. ACS_DECRYPTION_ERROR, Crypto Error.
1035	ACS error. ACS_ENCRYPTION_ERROR, Crypto Error.
1036	ACS error. ACS_BAD_SESSIONID_ERROR, bad session id
1037	ACS error. ACS_NO_AHAREC_ERROR, no CH data in AHA table
1038	ACS error. ACS_BAD_RANGE_ERROR, no brandinfo or range info
1998	ACS error. Unknown exception.
1999	ACS error. Last error.
2000	CAP error. Client authentication pages unable to connect to the ACS.
2001	CAP error. User pressed Cancel during Password Request phase
2002	CAP error. User pressed Cancel during hint answer request phase
2003	CAP error. User failed to supply correct hint answer
2004	CAP error. No Challenge returned by Arcot Authentication Server
2005	CAP error. Unable to connect to Arcot Authentication Server
2006	CAP error. User failed to supply EAccess Password
2007	CAP error. No VSDC Data returned from Chip Card Reader
2008	CAP error. No Authentication methods for card number
2009	CAP error. No Chip Card Plug-in on client computer
2010	CAP error. No EAccess Present
2011	CAP error. User Account has been disabled as Bank's PasswordUsagePolicy is 1
6000	Failed to get a merchant data string.

Table B-2 Processing Errors

Error Code	Description
6001	The merchant did not set an authorized purchase amount.
6002	The authorized amount contains characters other than numbers.
6003	The authorized amount is more than 12 characters in length.
6004	The authorized amount is 0.
6006	Missing country code.
6007	The country code contains characters other than numbers.
6008	The country code is not three characters in length.
6011	Missing currency code.
6012	The currency code contains characters other than numbers.
6013	The currency code is not three characters in length.
6016	The transaction date is missing.
6017	The transaction date contains characters other than numbers.
6018	The transaction date is not 6 characters in length.
6019	The date is invalid.
6021	The amount other value is missing.
6022	The amount contains characters other than numbers.
6023	The amount is longer than 12 characters in length.
6024	The amount other value is greater than 0. In Internet transactions, the amount other value must be 0.
6026	Missing XID.
6027	The XID contains characters other than hexadecimal numbers. hexadecimal numbers include: 0123456789abcdefABCDEF.
6028	XID is not 28 or 40 characters in length.
6029	XID base64 decoding failed.
6030	Base64 decoding did not return 20 characters as expected.
6035	Cannot call GetVSDCData() before calling SetMerchantData().
6040	Cannot call GetChipCardSecret() without the PIN.
6041	Could not load the eAccess wallet dll.

Table B-2 Processing Errors

Error Code	Description
6042	Could not call GetProcAddress() on GetSecretFromLibrary(), which retrieves the e-access secret password.
6043	Multiple instances of the browser have multiple instances of the chip card plug-in, and therefore the card was blocked by a mutex.
8000	HTTP Action is not 'POST'.
8001	Invalid HTTP header Content-Type.
8002	Invalid HTTP header Content-Length.
8003	HTTP Response is not 200 OK.
8004	Invalid HTTP Request header has been received.
8005	Invalid HTTP Response header has been received.
8006	No HTTP header Content-Length.
8007	Invalid XML message format.
8008	XML Message Root is not 3-D Secure.
8009	Invalid XML Element.
8010	Server and Client Protocol mismatch.
8011	Invalid Extension Critical value.
8012	Unable to handle Extension Element.
8999	Last XML error.

Default Configuration File Examples

This appendix contains examples of how the following *.ini configuration files appear after installation:

- `acs.ini`
- `acsclient.ini`
- `cap.ini`
- `comm.ini`
- `es.ini`
- `log.ini`

acs.ini Example

```
#
# Online Authentication Payment System parameters
# Arcot Systems's TransFort Product Configuration File
#
#####
#
# Arcot Access Control Server (ACS) Settings
#
#####

[arcot/vpas/acs]
#
# ACS Connection or Communication sub-system Settings
#
# DS Handler HTTP Channel number for ACS, default is 21
#HTTPDSChannel=21
HTTPDS1Channel=21
HTTPDS2Channel=22
HTTPDS3Channel=23
HTTPDS4Channel=24

# DS Handler Non-HTTP Channel number (ssl, tcp) for ACS, default
#is 20
DSChannel=20

# CAP Handler Channel number (ssl, tcp) for ACS, default is 24
CAPChannel=24

# Admin Handler Channel number (ssl, tcp) for ACS, default is 25
AdminChannel=25

# CAP Handler Channel number (http, https) for ACS, default is
#26
HTTPAdminChannel=26

#
# Configurable Connection Protocol parameters for ACS DS Handler
#
# Secure protocols are enabled by default.
# HTTPS is always Enabled Support...this cannot be disabled.

# Enable SSL Support for DS requests. Default is 1, enabled
```

```
EnableDSSSL=1

# Enable HTTP Support for DS requests. Default is 0, disabled
EnableDSHTTP=1

# Enable TCP Support for DS requests. Default is 0, disabled
EnableDSTCP=0


#
# Configurable Connection Protocol parameters for ACS CAP
#Handler
#

# Enable SSL Support. Default is 1, enabled
EnableCAPSSL=1

# Enable TCP Support. Default is 0, disabled
EnableCAPTCP=1

# Enable SSL Support. Default is 0, disabled
EnableAdminSSL=0

# Enable HTTPS Support. Default is 1, enabled
EnableAdminHTTPS=1

# ACS instance identifier for AAV computation
ACSIdentifierId=0


#
# Database Settings
#

# Database name. default is ArcotACSDatabase
DBName=ArcotACSDatabase

# Set this flag to 1 if you do not want to configure a backup
#database
# The default is 0 which means that we do have a backup database
NoBackupDB=1

# Backup database name. No defaults
# BackupDBName=ArcotACSDatabase

# Database user ID. No defaults
UserID=system
```

```
# Back up Database user ID. defaults is Primary dB's UserID
# BackupUserID=system

# Maximum number of database connections. Default 32
# MaxDBConns=32
MaxDBConns=50

# Minimum number of database connections to start with. Default
#16
MinDBConns=1

# By what amount should I increment if i hit a bottleneck.
Default 2
IncDBConns=2

# how many times to try to connect to db before abort ? default
#is 3 retries
MaxDBConnTries=3

# how many ms to sleep between each db connect retry ? default
#is 2000 ms
DBConnRetrySleepTime=2000

# which database? default is "oracledb"
DBType=oracledb

#this parameter specifies whether after a a failover, should the
#service again attempt to #connect to the primary DB. Default is
#0 , i.e the service will not attempt such a thing
DBAutoRevert=0

#this parameter specifies the time interval in seconds between
#attempts of the thread #connecting to the primary DB. Default
#is 3 sec
DBAutoRevertThreadTime=3

#To turn on Database logging messages. Default is 0; Set to 1 to
#enable it.
DBProfiling = 1

#
# ACS thread Settings
#

# Maximum threads allowed for ACS Admin Handler. Default 16
AdminMaxThreads=16
```

```
# Minimum threads allowed for ACS Admin Handler. Default 8
AdminMinThreads=8

# Maximum threads allowed for ACS DS Handler. Default 128
DSMaxThreads=128

# Minimum threads allowed for ACS DS Handler. Default 16
DSMinThreads=16

# Maximum threads allowed for ACS CAP Handler. Default 128
CAPMaxThreads = 128

# Minimum threads allowed for ACS CAP Handler. Default 16
CAPMinThreads = 16

#
# ACS Log Settings
#

# ACS Logfile name
LogfileName=logs/ArcotACSLog.txt

# the prefix for backup file. Part of log file name and
#date/time will be appended to this prefix
#RollOverLogPrefix=logs/Backup

# File size in bytes . This is 1MB
#MaxLogfileSize=1048576

# Logging level. Legal values are 1, 2 or 3
# default level is 1 or all messages (info, warning and fatal)
# level 2 implies warning and fatal messages will be logged
# level 3 implies only fatal messages will be logged
LogLevel=1

# Log file size checking frequency in minutes. Default is 15
#mins.
#LogFileSizeCheckFrequency=15

# Using nCipher for MasterKey
SoftMasterKey=false

# Number of Sessions to nCipher for
#encryption/decryption/signing
nCipherSessions=8
```

```
# Location of the nCipher PIN. The default is "file". If it is
#set to "prompt" the ACS
# comes up only with the admin listner and we will have to
#broadcast the PIN using ACSCClient -enable
PINLOCATION=file
#PINLOCATION=prompt

## new with patch 5.2.15:
# note that multiple pin locations can be specified for
#different crypto
# boxes by using arcot/vpas/acs/<cryptoModuleName>/PinLocation

# Default personal message to be used for a card holder during
#ADS
DefaultPM=

# Identifier for a particular ACS instance, in a multi-ACS
#deployment it is
# useful to set different values for this parameter for
#different ACS instances
InstanceId=3

#admin handler ssl certs
AdminSSLClientCACert=ssl/ClientRootCA.pem
AdminSSLServerCert=ssl/servercert.pem
AdminSSLServerKey=ssl/serverkey.pem

#cap handler ssl certs
CAPSSLClientCACert=ssl/ClientRootCA.pem
CAPSSLServerCert=ssl/servercert.pem
CAPSSLServerKey=ssl/serverkey.pem

#DS 1.01 handler ssl certs
#DS101SSLClientCACert=ssl/ClientRootCA.pem
#DS101SSLServerCertChain=ssl/ch2cert.pem
#DS101SSLServerKey=ssl/ch2key.pem

DS1SSLClientCACert=ssl/ClientRootCA.pem
#DS1SSLClientCACert=ssl/servercert.pem
DS1SSLServerCertChain=ssl/servercert.pem
DS1SSLServerKey=ssl/serverkey.pem

DS2SSLClientCACert=ssl/ClientRootCA.pem
DS2SSLServerCertChain=ssl/ch2cert.pem
DS2SSLServerKey=ssl/ch2key.pem

DS3SSLClientCACert=ssl/ClientRootCA.pem
```



```
DS3SSLServerCertChain=ssl/servercert.pem  
DS3SSLServerKey=ssl/serverkey.pem
```

```
DS4SSLClientCACert=ssl/ClientRootCA.pem  
DS4SSLServerCertChain=ssl/servercert.pem
```

acsclient.ini Example

```
#####
#
# ACSClient Settings
#
#####

[arcot/vpas/acsclient]

# Settings for DS Handler

# ACS Host name. If not set, default to localhost for DS to ACS
DSHost=localhost

# Backup Host name for DS to ACS
# DSBackupHost=localhost

# ACS Channel number for connecting to DSMgrHandler. If not set,
#default to 21
DSChannel=21

# Backup ACS Host Channel number for connecting to DSMgrHandler.
#If not set, default to 21
# DSBackupChannel=21

# Transport protocol to connect to ACS DSMgrHandler. Default to
#https.
# Valid values are http, https, ssl and tcp
DSTransport=http

# Backup Transport protocol to connect to ACS DSMgrHandler.
#Default to https.
# Valid values are http, https, ssl and tcp
# DSBackupTransport=https

# maximum connections to DS listener of ACS. Default is 128
DSMaxConns=128

# minimum connections to DS listener of ACS. Default is 16
DSMinConns=16

# Connection Timeout value to Connect to ACS (in seconds).
Default is 0 (infinity)
```

```
# Don't set this value too low as SSL connection setup is
#expensive.
# DSConnTimeout=0

# Timeout value for getting response from ACS (in seconds).
#Default is 0 (infinity)
# DSRespTimeout=0

# Settings for Admin Handler

# ACS Host name. If not set, default to localhost for DS to ACS
AdminHost=localhost

# Backup Host name for DS to ACS
# AdminBackupHost=localhost

# ACS Channel number for connecting to AdminMgrHandler. If not
#set, default to 26
AdminPort=9726

# Transport protocol to connect to ACS AdminMgrHandler. Default
#to https.
# Valid values are http, https, ssl and tcp
AdminTransport=https

# maximum connections to admin listener of ACS. Default is 128
AdminMaxConns=128

# minimum connections to admin listener of ACS. Default is 16
AdminMinConns=16

# Connection Timeout value to Connect to ACS (in seconds).
#Default is 0 (infinity)
# Don't set this value too low as SSL connection setup is
#expensive.
# AdminConnTimeout=0

# Timeout value for getting response from ACS (in seconds).
#Default is 0 (infinity)
# AdminRespTimeout=0

#Admin certificates
AdminServerCACert=ssl/ServerRootCA.pem
#AdminServerCACert=ssl/clientcert.pem
AdminClientCert=ssl/clientcert.pem
#AdminClientCert=ssl/serverkeyjunk.pem
```

```
AdminClientKey=ssl/clientkey.pem

#
#
# CAP Failover parameters
#
# ACS server hostname. Default is "localhost"
CAPHostName1=localhost
CAPHostName2=localhost

# Transport protocol to connect to ACS CAPMgrHandler. Default to
#ssl
# Valid values are tcp and ssl
CAPTransport1=tcp
CAPTransport2=tcp

# ACS Listener port number for connecting to CAPMgrHandler.
# If not set, default to 9724 or 9624 depending on value of
CAPTransport
CAPPortNo1=9624
CAPPortNo2=9624

# Connection Timeout value to Connect to ACS (in seconds).
#Default is 0 (infinity)
# Don't set this value too low as SSL connection setup is
#expensive.
#ACSConnTimeout1=0
#ACSConnTimeout2=2

# Timeout value for getting response from ACS (in seconds).
#Default is 0 (infinity)
#ACSRespTimeout1=0
#ACSRespTimeout2=2

# Number of Connections to ACS. Default is 128 and 16
CAPMaxConn1=128
CAPMaxConn2=128
CAPMinConn1=16
CAPMinConn2=16

# Remember to set parameters if using SSL connections between
# CAP & ACS:
# SSLCACert, SSLClientKey and SSLClientCert
# under arcot/comm section for SSL connections.
# This is typically set in comm.ini file

#CAP certificates
```

```
CAPServerCACert1=ssl/ServerRootCA.pem  
CAPClientCert1=ssl/clientcert.pem  
CAPClientKey1=ssl/clientkey.pem
```

cap.ini Example

```
#
#
# Arcot CLient Generic Page Filter/Extension Settings
# The information related to the ACS host and transport to be
used is picked up
# from arcot/vpas/acscclient section

[arcot/vpas/cap]
# Should always be 0, only for Debugging if it is missing it is
assumed to be 0.
Debug=1

#should be 0 if no pareq logging required,
#should be 1 if invalid pareq logging required
#should be 2 if all the pareq logging required
#please make sure that the cap debug is turned on (>0)
PareqLogLevel=0

#
# The following info assumes that the IIS directory is in
C:\Inetpub\wwwroot
# Must be set to the actual filesystem directory for acspage
# This directory contains all the templates and associated files
ExecPath=/project/sit/arcot/CAP/acspage

# Log file for all the CAP related messages
LogfileName=logs/ArcotCAPLog.txt

#
# This is the page that will be displayed by CAP in cases where
CAP can not
# communicate to ACS. Must be set to the actual path in the
filesystem
DefaultErrorPage=/project/sit/arcot/CAP/acspage/error.htm
```

comm.ini Example

```
# Communications parameters
#

[arcot/comm]
TCPBasePort=9600
UDPBasePort=9600
SSLBasePort=9700

SSLCACert=ssl/ServerRootCA.pem
SSLServerKey=ssl/serverkey.pem
SSLServerCert=ssl/servercert.pem
SSLClientCACert=ssl/ClientRootCA.pem
SSLClientKey =ssl/clientkey.pem
SSLClientCert=ssl/clientcert.pem

# when communicating with an external ssl server like globeset,
# which insists we
# present a client certificate chain, we should use the chained
# client pem file by uncommenting the line below. This is a
# benign change, i.e. even if you start using a chain within
# VPAS/Arcot, it works as before
#SSLClientCertChain=ssl/clientchain.pem

# Socket Recv timeout
# Default is no timeout (or a value of 0 secs)
# Socket Timeout for misc tools like dsclient/acsclient/ahs_stub
# in secs
SocketTimeout=0
```

es.ini Example

```
#
# Transfort Issuer Software
# ES parameters for connecting to IPGS
#

[arcot/vpas/es/ipgs]
Host=localhost
Port=1555

#Transport must be set to ssl when communicating with a live
IPGS system
Transport=tcp

#The following parameters are the complete paths to the
certificates and keys required
#to establish an SSL connection with IPGS. These files are
always required to be present
#on the ES file system if IPGS is being used. When you set the
Transport to "ssl", you must
#uncomment the parameters below.

#ClientCertPath=d:\program files\common files\arcot
shared\certificates\chain.pem
#ClientPrivKeyPath=d:\program files\common files\arcot
shared\certificates\arcotdsa.key
#CACertPath=d:\program files\common files\arcot
shared\certificates\serverca.pem

# The following value specifies the socket receive timeout in
milliseconds.
# If IPGS does not reply in this time interval you will get
error code 55 ie IPGS_RECV_ERROR
# If this value is not specified, we wait for the connection
till they time us out
SocketReceiveTimeoutMS=30000

[JNI/logger]
LogfileName=/project/sit/arcot/logs/ArcotJNILog.txt
BackupLogfile=/project/sit/arcot/logs/Backup
# File size in bytes
MaxLogfileSize=1048576
#LogLevel=0: No Logging
#LogLevel=1: Only Fatal Messages will be Logged
```



```
#LogLevel=2: Only Fatal and Warning Messages will be Logged  
#LogLevel=3: All Messages will be logged  
#Default value of LogLevel is 2  
LogLevel=3
```

log.ini Example

```
#
# Logging configuration
#

[arcot/logger]
LogfileName=logs/ArcotLog.txt
BackupLogfileName=logs/ArcotLogBackup.txt
# the prefix for backup file. Part of log file name and
# date/time will be appended to this prefix
RollOverLogPrefix=logs/Backup
# File size in bytes
MaxLogfileSize=1048576
# Logging level. 1 will log all the entries. Hierarchy is (info,
# warn, fatal i.e 1, 2 and 3)
LogLevel=1
```

Certificates Required

The Issuer Software uses many certificates in its communication to external components. This appendix lists all such certificates along with the Issuer Software component and the place where it is loaded.

The following table lists the certificates necessary to implement Arcot Transfort Issuer Software:

Table B-1 Certificate Requirements

Entity	Purpose	Certificates Required	Place Loaded
Access Control Server	CAP Certificates: Handling PAREq, Verify Password, Verify Hint Answer, etc.	SSL Server Certificates: CAPSSLClientCACert CAPSSLServerCert CAPSSLServerKey	acs.ini
	AHS Certificates: Handling receipts, Receipt Server certificates.	SSL Client Certificates: AHSCACertFile AHSClientCertFile AHSClientKeyFile	From the Update ACS Config page.
	Admin Handler Certificates: Handling Cache Refresh and Graceful shutdown	SSL Server Certificates: AdminSSLClientCACert AdminSSLServerCert AdminSSLServerKey	acs.ini
	Directory Server Certificates: Handling VReq	SSL Server Certificates: <i>For 1.0.1 and higher version:</i> DS101SSLClientCACert DS101SSLServerCertChain DS101SSLServerKey <i>For Multiple DS Listeners (N starts from 1):</i> DS<N>SSLClientCACert DS<N>SSLServerCertChain DS<N>SSLServerKey <i>Example:</i> DS1SSLClientCACert DS1SSLServerCertChain DS1SSLServerKey	acs.ini
Access Control Server	Signing Certificates: For signing PAREs	Signing Certificates: <i>For 1.0.1 and higher version:</i> SigningCertFile	From the Add FI Info page.
ACSClient	Admin Handler Certificates: Handling Cache Refresh, Graceful Shutdown.	SSL Client Certificates: AdminServerCACert AdminClientCert AdminClientKey	acsclient.ini

Table B-1 Certificate Requirements

Entity	Purpose	Certificates Required	Place Loaded
	CAP Certificates	CAPServerCACert1=ssl/ServerRootCA.pem CAPClientCert1=ssl/clientcert.pem CAPClientKey1=ssl/clientkey.pem	acsclient.ini
Data Upload Client	To authenticate the Enrollment Server	SSL Client Certificates: SSLCACert SSLClientKey SSLClientCert	comm.ini
Enrollment Server	To authenticate the DUC	SSL Server Certificates: SSLClientCACert SSLServerKey SSLServerCert	comm.ini
	To connect to IPGS. These certificates are required only for SSL connection.	SSL Client Certificates: ClientCertPath ClientPrivKeyPath CACertPath	es.ini

Appendix E

Restarting Services

There can be actions following which the ES or ACS or CAP services have to restarted to function as desired. The actions are listed according to the component which needs to be restarted or refreshed:

- [Actions requiring ES Restart](#)
- [Actions requiring ACS Restart](#)
- [Actions requiring CAP Restart](#)
- [Refreshing ACS Cache](#)
- [Refreshing ES Cache](#)

Actions requiring ES Restart

The actions which require the restart of the ES service are:

- New encryption keys are dynamically added to the security world.
- The `web.xml` file is modified.
- Changes to the MIPS or IPGS configuration parameters.
- Modification of the properties files like `staticmessages.properties`, etc.
- Addition or modification of directories as a part of customization changes.
- Database restart in case there is no backup database and `AutoRevert` is set to zero.
- When features like database failover or cache refresh are not used.

- Changes or modifications to ES configurations for any given range.
- Whenever the value of the `ESCacheRefreshFrequency` is changed from 0 to any valid value.

Actions requiring ACS Restart

The actions which require the restart of the ACS service are:

- Changes or modifications to the configuration information (like certificates or port numbers, database configuration, etc.) in the `acs.ini`, `comm.ini` files.
- When the cryptographic device process/hardware stops responding or all cryptographic device sessions are lost.
- Database restart in case there is no backup database and `AutoRevert` is set to zero.
- When features like database failover or cache refresh are not used.
- New encryption keys are dynamically added to the security world.
- Changes to the `SendReceipt` value in the `ACSConfig` page.

Actions requiring CAP Restart

The actions which require restart of the CAP are:

- Changes or modifications to the file system.
- Changes or modifications in the `cap.ini`, `acsclient.ini`, `comm.ini` and SSL certificates.

Refreshing ACS Cache

The actions following which an ACS cache refresh is required are listed below. See [“Refreshing ACS Cache” on page 222](#) for more information about ACS cache refresh.

- Any addition, deletion or change to Issuer configuration.
- Any addition, deletion or change to Range configuration.
- Any addition, deletion or change to CallOut configuration.
- Any modifications to ACS configuration parameters.

- Any modifications to the cardholder authentication parameters.
- Any addition or change to support for mobile devices
- Any addition, deletion or change to CAP templates/folders.

Refreshing ES Cache

The actions following which an ES cache refresh is required are listed below. See [“Admin/Enrollment Server Cache Refresh” on page 98](#) for more information about ES cache refresh.

- Any addition, deletion or change to Issuer configuration.
- Any addition, deletion or change to Range configuration.
- Any addition, deletion or change to CallOut configuration.

System Requirements Summary

This appendix provides a brief summary of the Issuer Software system software and hardware requirements. See the *Arcot TransFort Issuer Software Installation Manual* for more information.

This appendix provides system requirements and configuration details for the following Issuer Software components:

- **Issuer Software Database**
- **Access Control Server**
- **Client Authentication Pages**
- **Enrollment Server and Administrative Console**
- **Servlet Redirector**

Issuer Software Database

Table A-1 Database Requirements

Windows	Solaris	AIX
<ul style="list-style-type: none"> • Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 on Microsoft® Windows 2000 Advanced Server Service Pack 4 or Windows 2003. 	<ul style="list-style-type: none"> • Oracle® 8i and 9.2.0.1 on Sun® Microsystems Solaris™ 8 	<ul style="list-style-type: none"> • DB2 8.1 on AIX 5.a2
<ul style="list-style-type: none"> • Oracle® client driver version 10g, 9.2, 9.1, 9i, one of these in that order. 	<ul style="list-style-type: none"> • Oracle® client 8.1.7.1 	<ul style="list-style-type: none"> • Unix ODBC driver manager 2.2.3

Table A-1 Database Requirements

Windows	Solaris	AIX
	<ul style="list-style-type: none"> DataDirect 4.2 ODBC driver for Oracle 	

Access Control Server

Software Requirements

Table A-2 ACS Software Requirements

Windows	Solaris	AIX
<ul style="list-style-type: none"> Microsoft® Data Access Components 2.6 or higher 	<ul style="list-style-type: none"> Oracle® 8i on Sun® Microsystems Solaris™ 8 	<ul style="list-style-type: none"> DB2 8.1 on AIX 5.a2
<ul style="list-style-type: none"> Oracle® client 10g, 9.2, 9.1, 9i, one of these in that order. 	<ul style="list-style-type: none"> Oracle® client 8.1.7.1 	<ul style="list-style-type: none"> Unix ODBC driver manager 2.2.3
<ul style="list-style-type: none"> Oracle® ODBC Driver 10g, 9.2, 9.1, 9i, one of these in that order. 	<ul style="list-style-type: none"> DataDirect 4.2 ODBC driver for Oracle 	<ul style="list-style-type: none"> IBM DB2 ODBC driver

Hardware Requirements

The following hardware is required for ACS:

- A minimum of a Pentium-4 class, multi CPU, 2Mhz or greater system with 512 or greater MB RAM.
- A Host Security Module.** The ACS uses the Host Security Module (HSM) to verify cryptograms generated by EMV-compliant chip cards issued by an Issuer and to perform CVV calculations. Issuer Software currently supports the Thales e-Security HSM RG7000.

You may also need to configure your firewall to allow the HSM port to be accessible to the ACS. Multiple instances of ACS can share a single HSM.

See [Appendix A, “Setting Up Third-Party Hardware Components”](#), for more information on setting up the HSM.

**.Applicable only for Visa configurations.*

- *A Hardware SSL Accelerator.* Issuer Software currently supports nCipher™, payShield™ and IBM Crypto Device 4758. The hardware SSL accelerator is used to store sensitive keys. The hardware accelerator must have a SCSI interface, *not* PCI. Your computer must have a SCSI controller with a free SCSI ID. The nCipher accelerators are not supplied with SCSI controllers. If your computer does not have a SCSI interface, you need to fit a SCSI controller and install and test the appropriate driver software before installing the hardware accelerator.

You will need a dedicated hardware accelerator for every ACS machine (however, if the ACS and ES are installed on the same machine, they may share the same accelerator).

IMPORTANT:

In either a dual or multiple Application Tier server topology, all of the Application Tier components (all instances of ACS and ES and Administrative Console) need to share all cryptographic keys at all times from all machines. Therefore, careful planning must be done to ensure that all machines are part of the same nCipher security world. See [Appendix A, “Setting Up Third-Party Hardware Components](#) for information on setting up a security world.

Client Authentication Pages

The Client Authentication Pages (CAP) are Web server filters/extensions and template files. The following sections describe system requirements for installing the CAP.

NOTE:

You must install the ACS before you install the CAP. You will need to provide the ACS host name, transport, and port numbers during CAP installation.

Software Requirements

Table A-3 CAP Software Requirements

Windows	Solaris	AIX
<ul style="list-style-type: none"> • IIS 5.0 and above as web server 	<ul style="list-style-type: none"> • Apache 1.3.28 as web-server 	<ul style="list-style-type: none"> • IBM HTTP Server 1.3.19
<ul style="list-style-type: none"> • Microsoft Windows 2000 Advanced Server Service Pack 4 or Windows 2003 		

Hardware Requirements

The CAP Web server requires the following hardware:

- A minimum of a Pentium-4 class, multi CPU, 2Mhz or greater system with 512 or greater MB RAM.
- (Optional) Depending on the cardholder traffic anticipated on your Web server, you might want to consider installing a cryptographic hardware accelerator for the Web server for HTTPS communications. You can refer to the various cryptographic hardware accelerator vendors product documentations for further information on how this can help you.

Enrollment Server and Administrative Console

The Enrollment Server (ES) and the Administrative Console are Java applications designed to run on a Java servlet engine. The following sections describe system requirements for installing the Enrollment Server and Administrative Console.

Software Requirements

Table A-4 ES/Admin Software Requirements

Windows	Solaris	AIX
<ul style="list-style-type: none"> • Oracle Client 10g, 9.2, 9.1, 9i, one of these in that order. 	<ul style="list-style-type: none"> • DataDirect 4.2 ODBC driver for Oracle 	<ul style="list-style-type: none"> • Websphere Application Server 5.0 with latest patch fix.
<ul style="list-style-type: none"> • Sun® Microsystems JDK 1.5.x or 1.4.x 	<ul style="list-style-type: none"> • Websphere Application Server 5.0 with latest patch fix 	<ul style="list-style-type: none"> • Sun® Microsystems JDK 1.3.1_01
<ul style="list-style-type: none"> • Servlet Redirector 	<ul style="list-style-type: none"> • Sun® Microsystems JDK 1.3.1_01 	
<ul style="list-style-type: none"> • Tomcat 5.5.x or 4.1.x 		

Hardware Requirements

The Enrollment Server and Administrative Console require the following hardware:

- A minimum of a Pentium-4 class, multi CPU, 2Mhz or greater system with 512 or greater MB RAM.

- A Hardware SSL Accelerator. Issuer Software currently supports nCipher™, payShield™ and IBM Crypto Device 4758. The hardware SSL accelerator is used to store sensitive keys. The hardware accelerator must have a SCSI interface, *not* PCI. Your computer must have a SCSI controller with a free SCSI ID. The nCipher accelerators are not supplied with SCSI controllers. If your computer does not have a SCSI interface, you need to fit a SCSI controller and install and test the appropriate driver software before installing the hardware accelerator.

You will need a dedicated hardware accelerator for every ES machine (however, if the ACS and ES are installed on the same machine, they may share the same accelerator).

See [Appendix A, “Setting Up Third-Party Hardware Components”](#), for more information on setting up the hardware accelerator.

IMPORTANT:

In a dual or multiple Application Tier server topology, all the Application Tier components (all instances of ACS and ES and Administrative Console) need to share all cryptographic keys at all times from all machines. Therefore, careful planning must be done before hand to ensure that all machines are part of the same nCipher security world. See [Appendix A, “Setting Up Third-Party Hardware Components”](#) for information on setting up a security world.

- (Optional) Depending on the cardholder traffic anticipated on your Web server, you might also want to consider installing a cryptographic hardware accelerator for the Web server for HTTPS communications. You can refer to the various cryptographic hardware accelerator vendors’ product documentation for further information on how this can help you.

Servlet Redirector

Software Requirements

- Tomcat Redirector - for Windows
- Websphere’s Redirector for AIX and Solaris.

Configuring Issuer Software Components

This appendix provides a schematic representation to configure the different parameters for each component of the TransFort Issuer Software. The parameters are described for a basic three tier architecture of the Issuer Software. The *Arcot TransFort Issuer Software Introduction Manual* discusses more about the three tier architecture and the components of the Issuer Software.

This appendix provides system parameters and configuration details for the following Issuer Software components:

- [Access Control Server](#)
- [Configuring Database Failover](#)
- [Client Authentication Pages](#)
- [Configuring Receipts](#)
- [Configuring Crypto Devices](#)

Access Control Server

The ACS configuration parameters can be categorized into the following sections:

- Communication Channels
- Database Settings
- Timeout Parameters
- Wait Periods
- Threads and Connections

Communication Channels and Database Settings

The diagram below illustrates the communication channels from different components to the ACS. It also shows the database settings from the ACS. The table below describes the parameters in detail:

Figure G-1 ACS: Communication Channels and Database Settings

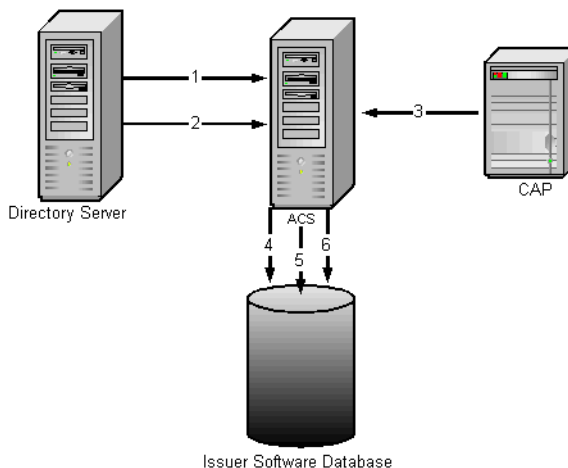


Table G-1 ACS: Communication Channels and Database Settings

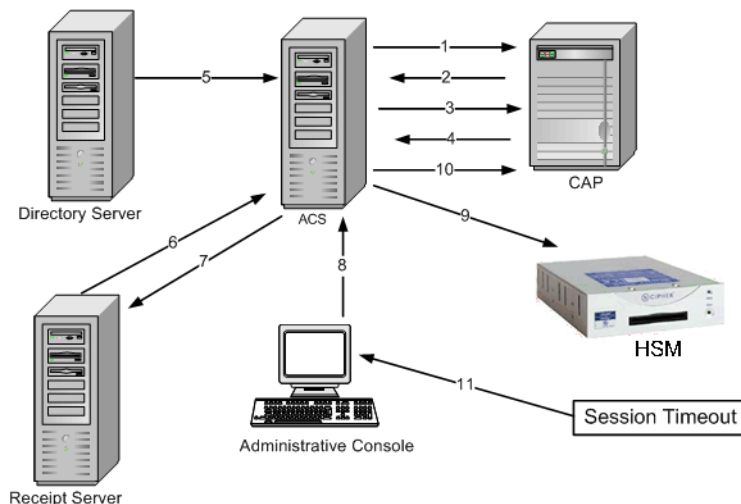
Parameter	Default Value and Place Loaded	Description
1. HTTPDSChannel	21 acs.ini	The offset to the base port used by the ACS DS Message Handler to listen to the HTTP or HTTPS requests coming from the DS. This is the channel used by default.
2. HTTPDS<N>Channel	No default acs.ini	The offset to the base port used by the ACS DS Message Handler to listen to the HTTP or HTTPS requests coming from the DS. This is the channel configured to support multiple DS listeners. See “Supporting Multiple DS Listeners,” for more information. Example: <pre> HTTPDS1Channel = 41 HTTPDS2Channel = 42 HTTPDS3Channel = 43 HTTPDS4Channel = 44 </pre>

Table G-1 ACS: Communication Channels and Database Settings

Parameter	Default Value and Place Loaded	Description
3. CAPChannel	24 acs.ini	The offset to the base port used by the ACS CAP Message Handler to listen to the SSL or TCP requests coming from the CAP.
4. MaxDBConns	32 acs.ini	The maximum number of connections that will be created between the ACS and the Issuer Software Database. Note: There is a limit to how many connections an Oracle database will allow and this limit overrides the MaxDBConn parameter. See your Oracle documentation for more information.
5. MinDBConns	1 acs.ini	The minimum number of connections to initially create between the ACS and the Issuer Software Database.
6. IncDBConns	2 acs.ini	The number of connections that will be created when a new connection is needed between the ACS and the Issuer Software Database.
MaxDBConnTries	3 acs.ini	The number of times the ACS will attempt to connect to the Issuer Software Database before aborting the connection.

Timeout Parameters

This section lists and describes the different timeout parameters in the ACS.

Figure G-2 ACS: Timeout Parameters**Table G-2 ACS: Timeout Parameters**

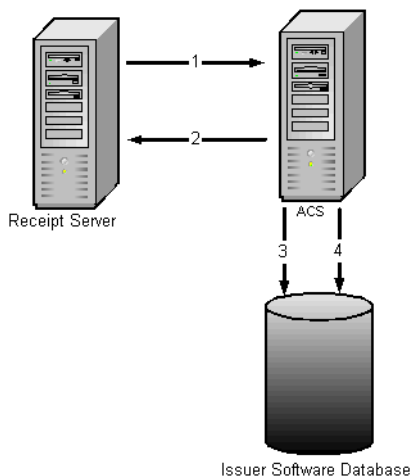
Parameter	Default Value and Place Loaded	Description
1. AdminConnTimeout	0 acscclient.ini	The number of seconds the ACSClient should wait when trying to connect to the ACS Admin Message Handler before the connection times out. 0 indicates no timeout and no attempt is ever made to connect to a backup host. If you comment out this parameter, the ACSClient assumes a default value of 10.
2. AdminRespTimeout	0 acscclient.ini	The number of seconds the ACSClient should wait before receiving a response from the ACS Admin Message Handler before the connection times out. 0 indicates no timeout. If you comment out this parameter, the ACSClient assumes a default value of 10.
3. ACSConnTimeout	2 acscclient.ini	The number of seconds the CAP or ACSClient should wait when trying to connect to the ACS CAP Message Handler before the connection times out. 0 indicates no timeout. If you comment out this parameter, the CAP or ACSClient assumes a default value of 0.

Table G-2 ACS: Timeout Parameters

Parameter	Default Value and Place Loaded	Description
4. ACSRspTimeou t	0 acsclient.ini	The number of seconds the CAP or ACSClient should wait before receiving a response from the ACS CAP Message Handler before the connection times out. 0 indicates no timeout.
5. ACSDSRcvTime out	0 Update ACSCConfig page	The number of seconds that the ACS will wait for a request from the DS before the connection will be closed. Default value is 0, which indicates the ACS will fall back to underlying TCP timeout.
6. ACSAHSRcvTim eout	0 Update ACSCConfig page	The number of seconds that the ACS will wait for a response from the AHS before the connection will be closed. Default value is 0, which indicates the ACS will fall back to underlying TCP timeout.
7. ACSAHSConnTi meout	0 Update ACSCConfig page	The number of seconds that the ACS will wait to connect to the AHS before the connection will be timed out. Default value is 0, which indicates the ACS will fall back to underlying TCP timeout.
8. ACSAdminRcvTi meout	0 Update ACSCConfig page	The number of seconds that the ACS will wait for a request from the Administrative Console before the connection will be closed. Default value is 0, which indicates the ACS will fall back to underlying TCP timeout.
9. Admin.Timeout	10 Update ESConfig page	The inactivity period in minutes after which the administrator's session from the console is timed out.
10. ACSCapRcvTi meout	0 Update	The number of seconds that the ACS will wait for a request from the CAP before the connection will be closed. Default value is 0, which indicates the ACS will fall back to underlying TCP timeout.

Wait Periods

The different wait periods in the ACS are illustrated in the figure below. The description is provided in the following table:

Figure G-3 ACS: Wait Periods**Table G-3 ACS: Wait Periods**

Parameter	Default Value and Place Loaded	Description
1. ReceiptWaitPeriod	10 Update ACSConfig page	The number of seconds the receipt dispatch thread will sleep between attempts to check the ACS receipt memory cache for new receipts.
2. ReceiptServerWaitPeriod	300 Update ACSConfig page	The number of seconds between ACS to AHS connection attempts.
3. DBConnRetrySleep Time	2000 acs.ini	The number of milliseconds to delay between attempts to connect to the Issuer Software Database.
4. DBAutoRevertThread Time	3 acs.ini	If DBAutoRevert=1 , this parameter specifies the number of seconds between attempts to connect to the primary database.

Threads and Connections

This section lists and describes all the connections and thread settings in the ACS.

Figure G-4 ACS: Threads and Connections

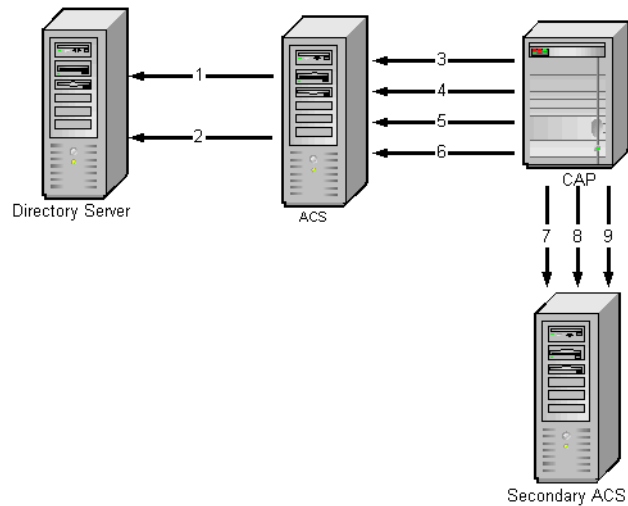


Table G-4 ACS: Threads and Connections

Parameter	Default Value and Place Loaded	Description
DSMaxThreads	128 acs.ini	The maximum number of threads that the ACS DS Message Handler will open in order to communicate with the DS or ACSClient.
DSMinThreads	16 acs.ini	The minimum number of threads that the ACS DS Message Handler maintains that are used to communicate with the DS or ACSClient.
CAPMaxThreads	128 acs.ini	The maximum number of threads that the ACS CAP Message Handler will open in order to communicate with the CAP or ACSClient.
CAPMinThreads	16 acs.ini	The minimum number of threads that the ACS CAP Message Handler maintains that are used to communicate with the CAP or ACSClient.
CAPMaxConn1	128 acsclient.ini	The maximum number of connections that the CAP stream pool should contain to connect to the primary ACS CAP Message Handler.

Table G-4 ACS: Threads and Connections

Parameter	Default Value and Place Loaded	Description
CAPMinConn1	16 acsclient.ini	The minimum number of connections that the CAP stream pool should contain to connect to the primary ACS CAP Message Handler.
Configuring Backup ACS		
AdminBackupHost	localhost acsclient.ini	The backup ACS host name for the ACSClient to use to connect to the ACS Admin Message Handler.
AdminBackupChannel	26 acsclient.ini	Deprecated parameter. The backup ACS channel for the ACSClient to use to connect to the ACS Admin Message Handler. If you comment out this parameter, the ACSClient assumes a default value of 25.
AdminBackupTransport	HTTPS acsclient.ini	The backup transport protocol the ACSClient will use to connect to the ACS Admin Message Handler.
CAPHostName2	localhost acsclient.ini	The secondary ACS host name for the CAP to use to connect to the ACS CAP Message Handler.
CAPTransport2	TCP acsclient.ini	The secondary transport protocol the CAP should use to connect to the ACS CAP Message Handler. If you comment out this parameter, the CAP or ACSClient assumes a default value of SSL.
CAPPortNo2	9624 acsclient.ini	The secondary port the CAP should use to connect to the ACS CAP Message Handler. If you comment out this parameter, the CAP or ACSClient assumes a default value of 9724 if CAPTransport2 is set to SSL, or 9624 if CAPTransport2 is set to TCP.
CAPMaxConn2	128 acsclient.ini	The maximum number of connections that the CAP stream pool should contain to connect to the secondary ACS CAP Message Handler.
CAPMinConn2	16 acsclient.ini	The minimum number of connections that the CAP stream pool should contain to connect to the secondary ACS CAP Message Handler.

Configuring Database Failover

It is always recommended that you configure a secondary database for the Issuer Software system. You need to configure the database for ACS and ES. This section describes the parameters you need to set to configure a backup database.

Figure G-5 Configuring Backup Database

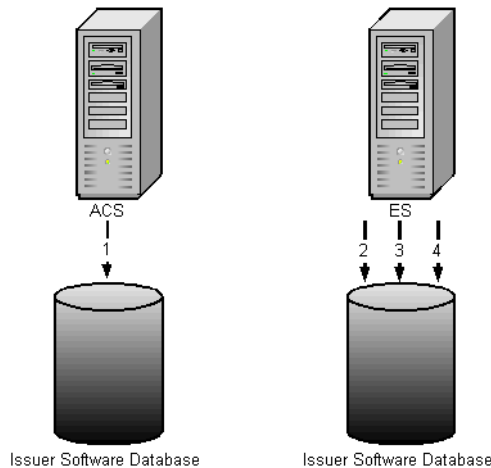


Table G-5 Configuring Backup Database

Parameter	Default Value and Place Loaded	Description
For ACS		
1. NoBackupDB	0 acs.ini	Indicates that a backup database is configured. Set to 1 if there is no backup database configured.
2. DBAutoRevert	1 acs.ini	Specifies whether or not the system will attempt to connect to the primary database after a failover occurs. Set DBAutoRevert=1 if you have a backup Issuer Software Database configured or if you want the ACS to try to connect to the database after a failover occurs.
3. DBAutoRevertT hread Time	3 acs.ini	If DBAutoRevert=1, this parameter specifies the number of seconds between attempts to connect to the primary database.

Table G-5 Configuring Backup Database

Parameter	Default Value and Place Loaded	Description
4. BackupDBName	No default acs.ini	The name of the ODBC System DSN pointing to the backup database hosting the Issuer Software data.
5. BackupUserID	No default acs.ini	The name of the backup user ID used by the ACS to access the Issuer Software Database
For ES		
1. db.count	2 web.xml	This parameter indicates the number of databases configured. You will need to edit this parameter in the web.xml and add the following parameters to configure the backup database.
2. db.1.driver	2 web.xml	The database driver configured for the backup database.
3. db.1.url	2 web.xml	The url for the backup database.
4. db.1.uid	2 web.xml	The user id for the backup database.
5. db.1.maxconn	2 web.xml	The maximum connections that will be created between ES and the backup database.
6. db.1.minconn	2 web.xml	The minimum connections that will be created between ES and the backup database.
7. db.1.inconn	2 web.xml	The number of connections that will be created when a new connection is needed between ES and the backup database.

Client Authentication Pages

The CAP is configured using the parameters described in the table below:

Table G-6 Configuring CAP

Parameter	Default Value and Place Loaded	Description
1. CAPChannel	24 acs.ini	The offset to the base port used by the ACS CAP Message Handler to listen to the SSL or TCP requests coming from the CAP.
2. AdminConnTimeout	0 acsclient.ini	The number of seconds the CAP or ACSClient should wait when trying to connect to the ACS Admin Message Handler before the connection times out. 0 indicates no timeout and no attempt is ever made to connect to a backup host. If you comment out this parameter, the ACSClient assumes a default value of 10.
3. AdminRespTimeout	0 acsclient.ini	The number of seconds the CAP or ACSClient should wait before receiving a response from the ACS Admin Message Handler before the connection times out. 0 indicates no timeout. If you comment out this parameter, the ACSClient assumes a default value of 10.
4. ACSConnTimeout	2 acsclient.ini	The number of seconds the CAP or ACSClient should wait when trying to connect to the ACS CAP Message Handler before the connection times out. 0 indicates no timeout. If you comment out this parameter, the CAP or ACSClient assumes a default value of 0.
5. ACSRespTimeout	0 acsclient.ini	The number of seconds the CAP or ACSClient should wait before receiving a response from the ACS CAP Message Handler before the connection times out. 0 indicates no timeout.
6. CAPMaxThreads	128 acs.ini	The maximum number of threads that the ACS CAP Message Handler will open in order to communicate with the CAP or ACSClient.
7. CAPMinThreads	16 acs.ini	The minimum number of threads that the ACS CAP Message Handler maintains that are used to communicate with the CAP or ACSClient.
8. CAPMaxConn1	128 acsclient.ini	The maximum number of connections that the CAP or ACSClient stream pool should contain to connect to the primary ACS CAP Message Handler.

Table G-6 Configuring CAP

Parameter	Default Value and Place Loaded	Description
9. CAPMinConn1	16 acsclient.ini	The minimum number of connections that the CAP or ACSClient stream pool should contain to connect to the primary ACS CAP Message Handler.
10. Debug	0 cap.ini	Indicates whether or not to write additional debug information to the <code>ArcACSLog.txt</code> log file. This parameter is for testing purposes only. Turning on this parameter can affect the performance of your CAP component resulting in lower throughput. After testing, turn this flag back to 0 and restart the web server.
11. ExecPath	c:\Inetpub\ wwwroot\acspage (for windows) or /opt/arcot/CAP/ acspage (for unix)	The path to the <code>acspage</code> folder. This directory is the root directory for all of the CAP templates and associated files. If you comment out this parameter, there is no default value.
12. LogFileName	logs/ArcotCAPLog.txt cap.ini	The path and filename to the log file for all messages related to CAP.
13. DefaultErrorPage	c:\Inetpub\ wwwroot\acspage\error .htm (for windows) or /opt/arcot/CAP/ acspage/error.h tm (for unix) cap.ini	The default error page displayed for any system error. For example, if the CAP not able to communicate with the ACS, the CAP displays this error page.

Configuring Receipts

This section describes the parameters you need to configure if you want to send the receipts generated by ACS to the receipt server. The following table describes these parameters:

Table G-7 Configuring Receipts

Parameter	Default Value and Place Loaded	Description
1. Send Receipt	0 Update ACS Config page	This parameter decides whether the system has to generate and send the transaction receipts to the receipt server. The possible values are: <ul style="list-style-type: none"> 0 - Create, but don't send the receipts 1 - Create and send the receipts
2. ReceiptQueueSize	100 Update ACS Config page	The number of active receipts kept in the ACS Receipt Handler queue before being sent to the Receipt Server.
3. ReceiptWaitPeriod	10 Update ACS Config page	The number of seconds the receipt dispatch thread will sleep between attempts to check the ACS receipt memory cache for new receipts.
4. ReceiptServerWaitPeriod	300 Update ACS Config page	The number of seconds between ACS to AHS connection attempts.
5. AHSLoginId	No default Update ACS Config page	The login ID for the ACS to use to access the AHS.
6. AHSPassword	No default Update ACS Config page	The password associated with the AHSLoginId.
7. ACSAHSRecvTimeout	0 Update ACS Config page	The number of seconds that the ACS will wait for a response from the AHS before the connection will be closed. Default value is 0, which indicates the ACS will fall back to underlying TCP timeout.
8. ACSAHSCnnTimeout	0 Update ACS Config page	The number of seconds that the ACS will wait to connect to the AHS before the connection will be timed out. Default value is 0, which indicates the ACS will fall back to underlying TCP timeout.

Table G-7 Configuring Receipts

Parameter	Default Value and Place Loaded	Description
9. AHSCACertFile	No default Update ACS Config page	The path and file name of the AHS Server CA Certificate.
10. AHSClientCert File	No default Update ACS Config page	The path and file name of the AHS Client SSL Certificate.
11. AHSClientKeyFile	No default Update ACS Config page	The path and file name of the AHS Client SSL key.
12. Receipt URL	No default Add FI Info page	<p>The URL to the Receipt Server or AHS that complies with the 3-D Secure protocol version 1.0.1 and version 1.0.2 DTD (or 1.0 messaging).</p> <p>If you don't want to send the receipts to any receipt server, you can enter <code>http://none</code> or <code>https://none</code> in this field. The ACS detects this url and does not attempt to send the receipt.</p>
13. InstanceId	0	<p>A parameter which can be used to identify any ACS instance. It is recommended that you provide unique values for every instance of ACS.</p> <p>The ACS while sending receipts will look for its unique InstanceId to send receipts generated only by it. The ACS instance is also displayed in the transaction reports, making it easier to trace the ACS to the transaction.</p> <p>IMPORTANT: In a farm of ACS servers, it is strongly recommended that each ACS have a different ID.</p>

Arcot Receipt Client

In addition to all the above parameters, you also have the option of using the command line tool Arcot Receipt Client to dispatch the receipts. See “,” for more information.

Configuring Crypto Devices

Issuer Software version 6.0 and higher allow you to configure multiple crypto devices. You can choose the crypto device to store:

- Sensitive Encryption keys
- Signing Keys
- Chip Card keys
- CVV2 or CVC2 key pairs for the CAVV or AAV generation
- HMAC key for AAV generation

You can configure separate devices for the bank and the range level. The configuration steps are simple and can be achieved from the console. You need to provide the device for issuer keys and CVV2/CVC2 keys at the issuer level and the signing keys, the CVV2/CVC2 keys and chip keys at the range level. For more details, see [“Determining the crypto device supported.”](#)

You can choose from the following crypto devices:

- nFast from nCipher
- Zaxus
- IBM 4578*
- IBM CCA*

**.Supported only on AIX systems*

The following table describes the parameters you have to configure for a crypto device:

Table G-8 Crypto Device Settings

Parameter	Default Value and Place Loaded	Description
HSM<N>DeviceName	No default Update ACS Config page	<p>The crypto devices supported by the ACS. The devices supported are:</p> <ul style="list-style-type: none"> • nfast - the nCipher SSL accelerator to store the sensitive bank keys, signing keys, etc. • ibm4758 - the PKSCS11 interface of the IBM 4758 crypto card. • cca - the CCA interface of the IBM 4758 crypto card. • zaxus - the Thales HSM to store the CVV keys. <p>NOTE: You must to configure one of the devices from this field for the ACS to connect to the device.</p>
Bank Key Module	No default Create Issuer page	<p>The crypto device used to store the bank encryption key. The options available are:</p> <ul style="list-style-type: none"> • nCipher - nShield • IBM Crypto Card - ibm4758 <p>NOTE: You must to configure the device you are selecting from the HSM<N>DeviceName field in the Update ACS Config page, before you configure the device here.</p>

Table G-8 Crypto Device Settings

Parameter	Default Value and Place Loaded	Description
Authentication Key Module	No default Create Issuer page	<p>The crypto device used to store the CVV/CVC2 keys. The options available are:</p> <ul style="list-style-type: none">• nCipher - payshield• IBM Crypto Card - cca <p>NOTE:You must to configure the device you are selecting from the HSM<N>DeviceName field in the Update ACS Config page, before you configure the device here.</p>
Singing Key Module	No default Add FI Info Page	<p>The crypto device used to store the signing key used for signing the PARes. The options available are:</p> <ul style="list-style-type: none">• nCipher - nShield• IBM Crypto Card - cca <p>NOTE:You must to configure the device you are selecting from the HSM<N>DeviceName field in the Update ACS Config page, before you configure the device here.</p>

Table G-8 Crypto Device Settings

Parameter	Default Value and Place Loaded	Description
Authentication Key Module	No default Add FI Info Page	<p>The crypto device used to store the CVV keys. The options available are:</p> <ul style="list-style-type: none"> • nCipher - payshield • Thales HSM • IBM Crypto Card - ibm4758 <p>NOTE:You must to configure the device you are selecting from the HSM<N>DeviceName field in the Update ACS Config page, before you configure the device here.</p>
Chip Key Module	No default Add FI Info Page	<p>The crypto device used to store the chip keys. This option is used when you use the chip card method for authentication. The options available are:</p> <ul style="list-style-type: none"> • nCipher - payshield • Thales HSM <p>NOTE:You must to configure the device you are selecting from the HSM<N>DeviceName field in the Update ACS Config page, before you configure the device here.</p>
host	No default zaxuscrypto.ini	The hostname or IP address of the primary HSM
port	No default zaxuscrypto.ini	The TCP port number of the primary HSM
backupHost	No default zaxuscrypto.ini	The hostname or IP address of the backup HSM
backupPort	No default zaxuscrypto.ini	The TCP port number of the backup HSM

Table G-8 Crypto Device Settings

Parameter	Default Value and Place Loaded	Description
headerLength	16 zaxuscrypto.ini	The header length, in bytes, for HSM commands
numConnections	2 zaxuscrypto.ini	The number of HSM connections to maintain
sharedLibrary	No Default zaxuscrypto.ini sppcrypto.ini pkcs11crypto.ini	You have to provide the shared library path to the .so file for the relevant crypto device.

Transfort Issuer Java APIs

TransFort Issuer is shipped with the following set of Java APIs:

- **verifyPassword**: This API authenticates the cardholder.
- **getCHProfile**: This API returns the cardholder profile.
- **updateCHProfile**: This API updates the cardholder profile.
- **Deploying Java APIs**: This API helps deploy a sample API.

NOTE: For more information on these Java APIs, refer to Javadocs that is shipped with the product.

verifyPassword

The `verifyPassword` API is used to authenticate the cardholder. This API uses `UserId`, `BankDirName`, and `CHPwd` as input parameters. The `CHPwd` parameter contains a list of passwords. This API returns the corresponding index value of the password that match with the cardholder. Alternatively, `PAN` and `BankDirName` parameter combination can be used to retrieve index value of password that match the cardholder value.

getCHProfile

The `getCHProfile` API is used to fetch locked or unlocked cardholder profiles. This API uses `UserId`, `BankDirName` and `CHPwd` as the input parameters. Alternatively, `PAN` and `BankDirName` parameter combination can be used to perform the operation.

NOTE: Invoke `verifyPassword` API, to ensure that the cardholder is not locked.

updateCHProfile

The `UpdateCHProfile` API is used to update the profile of a cardholder. This API can be performed only after the `getCHProfile` API.

Deploying Java APIs

The Java APIs, Javadocs, and the `test.jsp` file are deployed with TransFort Issuer application (ES/Admin component). The `test.jsp` file is a sample implementation file provided for developers to demonstrate the use of use these APIs.

Refer to “Installing ES/Admin Console” section of *Arcot TransFort Issuer Software Installation Guide* for more information.

Glossary

3-D Secure Protocol	An Internet-based protocol used to implement the MasterCard or Visa. Authenticated Payment Program for cardholder authentication (or identification) during an online purchase transaction.
AAV	Account Holder Authentication Value. Cardholder authentication data required by MasterCard for online transactions in which cardholder authentication has been successfully performed.
Abridged Enrollment	An Enrollment process that is used when cardholders are unable to enroll in the 3-D Secure program on their own. Alternatively, Issuers may choose to use this process for VIPs. The process is as follows: An Administrator manually adds a cardholder to the Issuer Software Database and gives the cardholder a temporary password to the Abridged Enrollment Web site. The cardholder accesses the Abridged Enrollment Web site and completes the Abridged Enrollment.
Acquirer	A MasterCard or Visa. Member financial institution that establishes a contractual service relationship with a merchant for the purpose of accepting MasterCard or Visa. cards. In 3-D Secure, determines whether merchant is eligible to participate. Performs traditional role of receiving and forwarding authorization and settlement messages (enters transaction into interchange).
ACS	The Access Control Server (ACS) is the component of the Issuer Software that enables verification of the identity of cardholders enrolled in the 3-D Secure program.
Admin Message Handler	Handles administration messages for the ACS from the ACSClient (regarding, for example, graceful shutdown or refreshing tables).
Administrative Console	Used by the different levels of Issuer Software administrators to perform system administration and cardholder management functions.

Administrator	This level of Issuer Software administrator is also known as a Customer Support Representative (CSR). An Administrator is responsible for administrative activities involving cardholders.
ADS	Activation During Shopping. A method of automatically enrolling cardholders while shopping, into the online authentication program.
Advanced Authorization	A feature for the administrators of the Issuer Software where one level of administrator can have extended functionality of administrators of lower levels.
AHS	The Authentication History Server (built and hosted by MasterCard or Visa.) stores a record for every attempted cardholder authentication by an ACS. Data includes the originating merchant requests and the authentication results.
ArcotIDs	Software smart cards that allow hardware level authentication in software form.
Attributes Step	A step in the ES where the cardholder provides personal information like name, date of birth, etc. during enrollment.
Authenticated Transaction	A e-commerce purchase where the cardholder is verified according to the 3-D Secure protocol to use the payment card.
Authentication	The process of verifying that the person making an e-commerce purchase is entitled to use the payment card.
Authorization	A process by which an Issuer, or a processor on the Issuer's behalf, approves a transaction for payment.
Auto FYP	A feature where the FYP feature is enabled automatically.
AVS	The Address Verification Service determines the identity of a cardholder based on whether or not the cardholder correctly enters the card billing address when enrolling in the 3-D Secure program.
BIN	Bank Identification Number. The first six digits of a payment card account number that uniquely identify the issuing financial institution.
CA	The Certificate Authority refers to the trusted entity that signs, issues, and revokes digital certificates.
CallOut	CallOuts are customized pieces of code that can be invoked for pre-defined events in the ACS and ES.
CAP	The Client Authentication Pages act as a user interface to the ACS. It displays a password pop-up page to cardholders who initiate 3-D Secure purchase transactions at participating merchant sites.
CAP Message Handler	Handles messages for the ACS from the CAP.

Cardholder	Party that holds a payment card, shops, provides card number and commits to payment.
CAVV	Cardholder Authentication Verification Value. A cryptographic value generated by the ACS to provide a way during authorization to rapidly validate the integrity of certain values copied from the Payer Authentication Response to the authorization request and to prove that authentication occurred.
certificate	A specially formatted block of data that contains a public key and the name of its owner. The certificate carries the digital signature of a CA to authenticate it.
certificate chain	An ordered grouping of digital certificates, including the Root certificate, that are used to validate a specific certificate.
chip card	A payment card with an integrated circuit chip that stores information about the account and user.
CVK	A Card Verification Key is a data-encrypting key in the HSM that is used to generate and verify card information (CVV output).
CVV	The Cardholder Verification Value is a verification algorithm used by the HSM to calculate CAVVs, or it can be the results of applying that algorithm to a particular card.
CVV2/CVC2	The Cardholder Verification Value 2 (CVV2) or the Cardholder Validation Code (CVC2) option determines the authentication status of a cardholder based on whether or not the cardholder correctly enters a three-digit verification code located on the signature panel on the back of the card.
DES	Data Encryption Standard is a publicly known cryptographic algorithm that converts plaintext to ciphertext using a 56-bit symmetric key.
digital certificate	See <i>certificate</i>
digital signature	An asymmetric cryptographic method whereby the recipient of the data can prove the origin and integrity of data, thereby protecting the sender of the data and the recipient against modification or forgery by third parties and the sender against forgery by the recipient.
DS	The Directory Server holds records of all card number ranges (but not individual card numbers, the names of the cardholders, or any other personal data) that are enrolled in the 3-D Secure program. It directs authentication requests from the Merchant Software to the ACS responsible for the account information for the cardholder being authenticated.
DS Message Handler	Handles messages for the ACS from the DS.

Dual Control	A feature that requires two administrators to log on to the Administrative Console to perform a specific task.
Enhanced Global Administrator	A global administrator having Advanced Authorization enabled. It means that a global administrator can have privileges of Issuer Administrators and CSR's.
Enrollment	The act of registering cardholders into the MasterCard or Visa. Authentication Payment Program.
ES	The Enrollment Server is the Issuer Software component used to enroll cardholders in the MasterCard or Visa. Authentication Payment Program.
External Verification	Cardholder identity verification during enrollment that is conducted by an Issuer's own authentication system.
FI	In terms of the Issuer Software, Financial Institution refers to the establishment responsible for facilitating customer-initiated transactions for the extension of credit. Also referred to as an Issuer.
FYP	Forgot Your Password - a feature where the cardholder can have alternate methods of authentication when the actual password is forgotten.
Global Administrator	An Issuer Software administrator responsible for setting up Issuer accounts and configuring the Issuer Software.
Hardware Accelerator	A hardware component used by the Issuer Software to store Master Keys, Issuer Encryption Keys, and Signing Keys and to perform cryptographic calculations involving those keys.
Hint Question/Answer	Hint is a question configured by the cardholder, which can be used when the cardholder clicks on FYP. The answer is also set by the cardholder.
HMAC	The Keyed-Hash Message Authentication Code is an option for Issuers to use to calculate CAVVs and AAV's.
HSM	The Host Security Module is used by the Issuer Software to enable CVV calculations and chip card support.
Identification Step	The first step in the enrollment process in the ES. This is the step where the cardholder provides the card number.
In Wallet Score	A numerical score between 1 - 999 issued by a third-party authentication service that indicates the cardholder's authentication status.
Internal Verification	Cardholder identity verification during enrollment that is conducted against the Issuer Software Database.
IPGS	The Internet Payment Gateway System processes payment authorizations for online purchases.
Issuer	In terms of the Issuer Software, Issuer refers to the establishment responsible for facilitating customer-initiated transactions for the extension of credit. Also referred to as Financial Institution.

Issuer Administrator	An Issuer Software administrator responsible for managing Administrator accounts, managing other Issuer Administrator accounts, and for configuring Issuer-specific enrollment parameters.
Issuer Encryption Keys	Triple DES keys used to encrypt and decrypt data for the different Issuers hosted by the Issuer Software.
Issuer Questions	Issuer configured questions to verify the cardholder before authentication. Standard questions include asking for the cardholder's mother's maiden name, city of birth, and so on.
Issuer Software Database	The persistent database storage that contains all the data required by an installation of the Issuer Software. This includes cardholder data as well as some component configuration information.
LMK	The Local Master Keys are DES or triple DES keys that encrypt the keys stored on the HSM.
Master Administrators	A pair of Issuer Software administrators who initialize the Issuer Software after installation and set up the first Global Administrators.
Master Key	A triple DES key that is used to encrypt values such as the Issuer Encryption Key labels, the Issuer Software Database user name and password, and so on. There is only one Master Key per Issuer Software deployment.
MDK	The Master Derivation Key on the HSM is used to enable chip card support. In the Issuer Software, this value is referred to as the HSM Variant.
merchant	Entity that contracts with an Acquirer to accept MasterCard or Visa. cards. Manages the online shopping experience with the cardholder, obtains card number, then transfers control to the Merchant Server Plug-in, which conducts payment authentication.
Merchant Server	The Merchant Server handles inter-component messaging between the Merchant Software and the other components in the 3-D Secure system.
Merchant Software	The Merchant Software plugs into the Web Server and is used to trap purchase requests. This is also known as the Merchant Filter or Merchant Plug-in. The Merchant Software also includes an SDK.
nCipher PIN	The operator pass phrase for an operator card included in the nCipher security world used by the Issuer Software. Each operator card in the nCipher security world may have a different PIN.
On-Behalf-Of Host	A third-party organization that hosts the Issuer Software for Issuers.
Online Authentication Program	A method which verifies and authenticates a online transaction in compliance to the 3-D Secure protocol.

Online Payer Authentication Program	One of the programs of the MasterCard or Visa Secure e-Commerce Initiative, this program includes two authentication protocols: 3-D Secure and 3-D SET
Out Wallet Score	A percentage score issued by a third-party authentication service that indicates the percentage of third-party enrollment questions the cardholder answered correctly.
PAN	The Primary Account Number is the number on the payment card that identifies the cardholder's account.
PAReq	The Payer Authentication Request is triggered by a positive response from the ACS regarding cardholder status. This message is sent by the Merchant through the cardholder's browser to the ACS.
PARes	The Payer Authentication Response is a message generated by the ACS in response to a PAReq. Regardless of whether authentication is successful, the ACS generates a PARes message and signs it with its MasterCard or Visa.-branded signing certificate, then sends the message back to the Merchant Software through the cardholder's browser.
Passphrase	The encryption/decryption key used to encrypt/decrypt data during upload.
Pre- Authorization	Pre-Authorization program (also known as \$1 authorization) determines the authentication status of a cardholder based on whether or not a one dollar test purchase authorization is accepted by the cardholder's credit card account.
ProxyPAN	A unique identifier of the card number. This is the value sent in all the external communications instead of the actual card number. The value generated here is always the same for a card number.
Receipt	A receipt is an acknowledgment of an authenticated online payment
Re-enrollment	An alternate method of verifying the cardholder other than password. You can use this method to verify and then allow them to reset the password.
RSA	The Rivest-Shamir-Adleman method is the most commonly used public key algorithm for encryption and digital signatures.
Servlet Container	The Issuer Software uses the Tomcat servlet container to invoke the Enrollment Server and Administrative Console.
Servlet Redirector	A Web server filter that directs requests or user input from a browser to the servlet container and returns content to the browser. The Servlet Redirector directs both cardholder enrollment input and Administrative Console input to the servlet container.
Signing Keys	Private RSA keys used by the ACS to sign Payer Authentication Responses (PARes).

SSL	Secure Sockets Layer. A cryptographic protocol to confidentially transmit information over open networks like the Internet.
Third-Party Verification	Cardholder identify verification during enrollment that is conducted by a third-party such as Experian.
Transaction ProxyPAN	Another identifier for the card number. There is a unique value generated for every transaction.
Verify Enrollment Request	<i>VEReq.</i> Message from MasterCard or Visa. Directory to ACS, asking whether authentication is available for a particular card number.
Verify Enrollment Response	<i>VERes.</i> Message from ACS or MasterCard or Visa. Directory, telling whether authentication is available.

Index

Symbols

\$1 Authorization
 configuring 111

A

AAV

 ACS IdentifierID 193

Abridged Enrollment 47

Abridged Registration

 temporary password duration 64

ACS

 ACSIIdentifierID 193

 InstanceId 193

 list of processing error codes for 258–261

 list of transaction details status codes for 256–257

 log file settings in acs.ini 190–192

 message handlers in 185

 refreshing cache for 222–224

 updating global configuration of 140–144

 updating server installation 184–192

ACS Identifier 193

ACS Instance Identifier 193

acs.ini 184–192

 CAP, Admin and DS message handler certificate settings 195–197

 communication channel settings 184–185

 database settings 186–188

 example of installation default 264–269

 message handler connection protocol settings 185–186

 nCipher settings 192

 thread settings 189–190

ACSClient

 performing a graceful shutdown 224–226

 refreshing cache 222–224

 settings in 222–226

ACSClient

 transmitting nCipher PIN 226

acsclient.ini

 example of installation default 270–273

 settings in 198–201

 updating for use with ACSClient 222

acspage directory 89, 146, 150, 203, 204

Adaptive ADS 172

 Cancelling 174

adding

 CAP template customization to Issuer account 146–149

 cardholder accounts 49–51

 financial institution information to Issuer account 85–94

 support for mobile phones to Issuer account 145

Admin Message Handler 185, 186, 189, 198–199

Administrative Console

 basic tasks 19–22

 logging in 19–20

 logging out 20

 setting timeout for 211

 user interface 17–18

Administrator

 about 10

 logging out of Admin Console 20

Administrator accounts

 configuring privileges for 36

 creating 26

 enabling or disabling 32

 specifying password policy for 34–35

 updating privileges for 30

Administrator Activities Log 40–41

administrator group hierarchy 8–16
 Administrator Report Access Log 40
 administrator, common
 changing password 20–21
 dual control 15
 exporting reports to file 22–23
 password policies 16
 privileges 15
 updating report profile 21
 ADS
 Adaptive ADS 172
 Issuer Activation 170
 OptIn 162
 Purchase Attempts 178
 Secondary Cardholder 164
 Summary Cardholder Experience 175
 AHS
 certificates 141, 144, 306
 specifying login parameters for ACS 141, 305
 apache_log.txt 217
 ArcACSLog.txt 203
 ArcotACSLog.txt 190–192, 217
 ArcotLog.txt 209
 Attributes Step 106
 Auto Enrollment 47
 Issuer Activation 48
 Optin 48
 Purchase Attempts 48
 AVS
 configuring 112
 defining policy for Issuer account 100, 102

B
 backup ACS 89
 backup database 187
 inserting user name and password into vspas-
 wd.ini 228–229
 specifying for ACS 186–188
 specifying for ES 212–214
 branding URL 89

C

cache
 refreshing 222–224
 Cache Refresh
 ES 98
 CallOuts
 Add CallOut Configuration 119
 Add Issuer CallOut 121
 Configuring 118–123
 Update CallOut Configuration 121
 cancelling cardholder accounts 58
 CAP
 customizing 89, 146–149, 150–151
 defining failover for 200
 CAP Message Handler 185, 186, 190, 197, 200–
 201
 cap.ini
 example of installation default 274
 settings in 203
 Card range name 86
 cardholder accounts
 adding 49–51
 cancelling 58
 lock/unlock 55
 resetting passwords 57
 updating responses to Issuer questions 56
 viewing information 51
 cardholder enrollment. *See* Enrollment
 Cardholder fields
 Standard Enrollment 106
 cardholder password
 temporary password duration 64
 cardholder password policy
 temporary duration 64
 cardholder verification policy, defining 100, 101
 Cardholder Verification Value. *See* CVV
 CardholderFields
 Abridged Enrollment 106
 catalina_log.txt 217
 certificates
 AHS 141, 144, 306

- Signing 70
- chip card
 - enabling support 90
 - enabling support in HSM 244–245
- comm.ini
 - example of installation default 275
 - settings in 205–206
- communication channel settings in acs.ini 184–185
- Configure Enrollment Process 105–117
 - Attributes 110
 - configuring range groups vs specific range 103
 - Fields 106
 - Issuer Questions 115
 - Order 108
 - Password 113
 - Question Policy 116
- Configuring
 - Adaptive ADS 172
- configuring
 - cardholder password policy 113
 - Enrollment Server Parameters for Issuer 62–64
 - Global Administrator privileges 36
 - HSM 242–243
 - Issuer Software 96–144
 - range group or a specific range 103
- Configuring Issuer Parameters 62–64
- creating
 - Administrator accounts 26
 - Global Administrator accounts 27–28
 - Issuer account 74–77
 - Issuer Encryption Keys 236
- CSR Administrator. *See* Administrator
- CSV report format 22–23
- customizing
 - CAP 89, 150–151
 - Enrollment site 124
 - Enrollment site graphics 126–129
 - Enrollment site messages 130
 - Enrollment site text 125–126
 - ES User interface templates 124
 - Issuer account directory for Enrollment site 72
 - new ES directory structure 125

- CVC 2
 - defining policy for Issuer account 102
- CVC 2 Policy 101
- CVC2
 - configuring 112
- CVK pair 75, 91, 244
- CVV
 - about 70
 - enabling calculations in HSM 244
 - key pair values
- CVV2
 - defining policy for Issuer account 101

D

- database
 - settings in acs.ini 186–188
- date separators, defining 64
- DBUtil 227–230
 - inserting backup database user name and password into vspawd.ini 228–229
 - updating the Master Key label 227
 - using additional options 229
- determining
 - cardholder identity verification policy for MasterCard 101
 - cardholder identity verification policy for Visa configurations 100
- disabling
 - Administrator accounts 32
- DS Message Handler 185, 189
- dual control
 - about 15
 - logout secondary 20

E

- enabling
 - Administrator accounts 32
 - chip card support in HSM 244–245
 - CVV calculations in HSM 244
- Encryption Keys. *See* Issuer Encryption Keys

Enrollment

- Abridged 47
- Attributes 110
- Auto 47
- directory 110
- fields 106
- Secondary Cardholder 164
- Standard 46–47
- Steps 108
- Template 111

Enrollment fields 106

Enrollment sequence 108

Enrollment Steps 108

Enrollment Web site

- customizing 124
- customizing graphics for 126–129
- customizing messages in 130
- customizing text in 125–126

error codes

- processing errors 258–261
- transaction details status codes 256–257

ErrorMessage.properties 130

ES

- Attributes 110
- Cache Refresh 98
- enabling or disabling IPGS 96
- log file 217
- updating global configuration 96

es.ini

- example of installation default 276
- settings in 207–208

exporting reports to file 22–23

F

failover

- database 187
- defining backup ACS for Issuer account 89
- defining CAP to ACS communication 200

FI BIN 86

G

generating an Issuer Encryption Key 68–69

Global Administrator

- about 9
- logging in to Admin Console 19
- logging out of Admin Console 20

Global Administrator accounts

- creating 27–28

graceful shutdown 224–226

graphics

- customizing for CAP 150–151
- customizing for Enrollment site 126–129

groups, administrator 8–16

H

hardware accelerator

- adding to security world 250
- setting up 246–250

HSM

- configuring 242–243
- defining MDK for Issuer account 91
- enabling chip card support 244–245
- enabling CVV calculations 244
- setting up 242–245
- setting up key management 243–244

I

Identification Step 106

InstanceId 193

IPGS

- certificate settings in es.ini 207–208
- enabling or disabling for Enrollment Server 96

isapi_redirect.log 217

Issuer

- determining passphrase 69
- selecting preferred locale 59
- updating 78

Issuer account 62–64

Issuer account directory 74

- creating 72

- Issuer Accounts
 - defining questions for 115
- Issuer accounts
 - adding support for mobile phones to 145
 - creating 74–77
 - creating Issuer account directory for 72
 - defining authentication parameters for cardholders 90
 - defining backup ACS for 89
 - defining customized CAP templates for 146–149
 - defining HSM MDK for 91
 - defining image files for 89
 - defining Signing certificates for 90
 - obtaining Signing certificate for 70
- Issuer Administrator
 - about 9
 - logging in to Admin Console 19
 - logging out of Admin Console 20
- Issuer Administrator Activities Log 42
- Issuer Data Policy
 - Question Policy 116
- Issuer Encryption Keys
 - about creating 68–69
 - adding to security world 250
 - creating 236
 - relationship with nCipher 247–249
- Issuer Questions
 - configuring 115
- Issuer questions
 - updating cardholder responses to 56
- Issuer Software
 - global configuration 96–144
- Issuer Software Database
 - backup database 187
 - settings in acs.ini 186–188
 - specifying a backup for ES 212–214

J

- jasper.log 218–219

K

- Key Management 225
 - ACS 225
 - ES 226
 - ES nCipher Settings 215
- key management, setting up 243–244
- keys
 - AHS 144
 - Issuer Encryption Keys, creating 68–69, 236
 - Master Key
 - updating label for 227
 - relationships with nCipher 247–249

L

- localhost_access_log.txt 218
- localhost_log.date.txt 218
- lock cardholder 55
- lock password, defining for cardholder authentication 64
- log files 217
 - apache_log.txt 217
 - ArcotACSLog.txt 217
 - ArcotCAPLog.txt 204
 - ArcotLog.txt 209
 - catalina_log.txt 217
 - changing ES log file location 212
 - ES log file 217
 - isapi_redirect.log 217
 - localhost_access_log.txt 218
 - localhost_log.date.txt 218
 - message levels 191, 192, 210
 - settings in acs.ini 190–192
- log.ini
 - example of installation default 278
 - settings in 209–210
- logging in to Administrative Console 19–20
- logging out
 - of Administrative Console 20
 - of dual control tasks 20

M

managing

- cardholder accounts 49–59
- Global Administrator accounts 37–38

Master Administrator

- about 8
- logging in to Admin Console 20
- logging out of Admin Console 20

Master Key

- relationship with nCipher 247–249
- updating label for 227

MDK 244–245

message files, customizing 130

message handlers

- Admin 185, 186, 189, 198–199
- CAP 185, 186, 190, 200–201
- certificate settings in acs.ini 195–197
- connection protocols 185–186
- DS 185, 189
- in ACS 185

mobile support

- adding new phones to 145
- defining for Issuer account 87

modifying the Servlet Redirector log settings 218–219

Multiple DS

- Configuring Certificates 196
- Starting 195
- Support 194

Multiple Locale

- Setting Preferred Locale for a Card locale

Setting Card Locale 59

N

nCipher

- adding box to security world 250
- adding Issuer Encryption keys to 250
- keys stored in 247–249
- setting up 246–250

setting up security world 246–247

settings in acs.ini 192

nCipher PIN

transmitting 226

O

obtaining

- AHS certificates and key 144
- Receipt Server information 71

Order

- Abridged Enrollment 108
- Standard Enrollment 108

P

PAN 87

passphrase

determining 69

password policy

- about 16
- specifying for Administrators 34–35

passwords, administrator

changing own 20–21

passwords, cardholder

- resetting 57
- temporary 49

performing

- a graceful shutdown 224–226
- Issuer Account pre-setup tasks 68–73

personal message 47

PK11 Util 231–237

PK11Util

- creating 236–??
- creating Issuer Encryption Keys ??–236

privileges, administrator

- about 15
- configuring for 36
- updating for an Administrator 30
- updating for Global Administrator 30

processing error codes 258–261

purchase transactions

viewing for cardholder 51

Q

Question Policy
 configuring 116

R

Receipt Server
 obtaining information about 71
Receipts
 Instance Id 193
records per report page 21, 63
refreshing ACS cache 222–224
Registration. *See* Enrollment
report profile, updating administrator 21
reports
 Administrator Activities Log 40–41
 Administrator Report Access Log 40
 defining time stamps for 63
 exported encoding format 75
 exporting to file 22–23
 Global Administrator Report Access Log 43
 Issuer Administrator Activities Log 42
 Issuer Administrator Report Access Log 41
 specifying time zone for Issuer account 74
resetting
 cardholder passwords 57
ring buffer size 141

S

Secondary Cardholder
 enrolling 164
SecureCode
 removing from cardholder account 58
Security
 Master Key 225
security world
 adding an accelerator to 250
 adding new Issuer keys to 250

 setting up 246–247
server.xml 218–219
Servlet Redirector
 modifying log settings 218–219
servlet.log 218–219
session timeout, setting 211
setting up
 HSM 242–245
 Issuer accounts 67–145
 nCipher 246–250
shutdown, graceful 224–226
Signing certificates
 defining for Issuer account 90
 obtaining for Issuer 70
Signing Keys
 relationship with nCipher 247–249
specifying
 Administrator password policy 34–35
specifying a backup database 212–214
Standard Enrollment 46–47
StaticMessages.properties 130
status codes
 transaction details 256–257

T

templates, CAP 146–149
temporary cardholder passwords 49, 57
temporary password duration 64
thread settings in acs.ini 189–190
Threads
 Admin Message Handler 189
 CAP Message Handler 190
 DS Message Handler 189
timeout, setting session 211
timestamps
 authentication transactions 64
 in reports 63
tomcat.log 218–219
transaction details status codes 256–257

U

unlock cardholder 55

Update issuer 78

updating

ACS configuration 140–144

Administrator Privileges for an Administrator
30

ES configuration 96

financial institution information for Issuer ac-
count 94

Master Key label 227

privileges for a Global Administrator 30

V

viewing

cardholder account information 51

Global Administrator Report Access Log 43

Global Administrator Reports

Global Administrator Activities Log 42

Issuer Administrator Report Access Log 41

Issuer Administrator reports 39–42, 66

vpaspwd.ini 227

deleting, inserting, and updating values in 229

inserting backup database user name and pass-
word into 228–229

specifying backup database in 212–214

updating Master Key label in 227

W

Web site, Enrollment

customizing graphics for 126–129

customizing messages in 130

customizing new ES 124

customizing text in 125–126

web.xml

changing ES log file location in 212

nCipher Settings 215

specifying a backup database in 212–214

specifying session timeout in 211